第一章　基本概念

§1．集　　合

1．$B \subset A$，但B不是A的真子集，这个情况什么时候才能出现？

解　由题设以及真子集的定义得，A的每一个元都属于B，因此$A \subset B$．于是由

$$B \subset A \qquad A \subset B$$

得$A=B$．所以上述情况在$A=B$时才能出现。

2．假定$A \subset B$，$A \cap B=$？$A \cup B=$？

解　（i）　由于$A \subset B$，所以A的每一个元都属于B，即A的每一个元都是A和B的共同元，因而由交集的定义得

$$A \subset A \cap B$$

但显然有

$$A \cap B \subset A$$

所以

$$A \cap B=A$$

（ii）　由并集的定义，$A \cup B$的每一元素都属于A和B之一；但$A \subset B$，所以$A \cup B$的每一元素都属于B：

$$A \cup B \subset B$$

另一方面$B \subset A \cup B$，所以$A \cup B=B$。

§ 2. 映 射

1. $A=\{1, 2, \cdots, 100\}$. 找一个$A\times A$到A的映射。

解 用(a, b)表示$A\times A$的任意元素，这里a和b都属于A。按照定义做一个满足要求的映射即可，例如

Φ: $$(a, b)\longrightarrow a$$

就是这样的一个，因为Φ替$A\times A$的任何元素(a, b)规定了一个唯一的象a，而$a\in A$。

读者应该自己再找几个$A\times A$到A的映射。

2. 在你为习题1所找到的映射之下，是不是A的每一个元都是$A\times A$的一个元的象？

解 在上面给出的映射Φ之下，A的每一个元素都是$A\times A$的一个元的象，因为(a, b)中的a可以是A的任一元素。

你自己找到的映射的情况如何？有没有出现A的元素不都是象的情况？假如没有，找一个这样的映射。

§ 3. 代数运算

1. $A=\{$所有不等于零的偶数$\}$。找一个集合D，使得普通除法是$A\times A$到D的代数运算。是不是找得到一个以上的这样的D？

解 一个不等于零的偶数除一个不等于零的偶数所得结果总是一个不等于零的有理数。

所以取

$$D=\{\text{所有不等于零的有理数}\}$$

普通除去就是一个 $A\times A$ 到D的代数运算。

可以找得到一个以上的满足要求的 D。读者可以自己找几个。

2. $A=\{a,\ b,\ c\}$。规定A的两个不同的代数运算。

解 （i）我们用运算表来给出 A的一个代数运算：$\circ$

	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

按照这个表，通过$\circ$，对于A的任何两个元素都可以得出一个唯一确定的结果 a 来，而 a 仍属于A。所以$\circ$是A的一个代数运算。

这个代数运算也可以用以下方式来加以描述

$\circ$: $\quad (x,\ y)\longrightarrow a=x\circ y \quad$ 对一切 $x,\ y\in A$

（ii） 同理

$\circ$: $\quad (x,\ y)\longrightarrow x=x\circ y \quad$ 对一切 $x,\ y\in A$

也是A的一个代数运算．读者可用列表的方法来给出这个代数运算。

读者还应自己给出几个A的代数运算。

§4. 结合律

1. $A=\{\text{所有不等于零的实数}\}$．$\circ$是普通除法：

$$a \circ b = \frac{a}{b}$$

这个代数运算适合不适合结合律？

解 这个代数运算 $\circ$ 不适合结合律．例如，

当

$$a = 4 \qquad b = c = 2$$

时

$$(a \circ b) \circ c = (4 \circ 2) \circ 2 = \frac{4}{2} \circ 2 = \frac{2}{2} = 1$$

$$a \circ (b \circ c) = 4 \circ (2 \circ 2) = 4 \circ \left(\frac{2}{2}\right) = \frac{4}{1} = 4$$

所以当 a，b 和 c 取上述值时

$$(a \circ b) \circ c \neq a \circ (b \circ c)$$

2． $A = \{$所有实数$\}$．代数运算

$\circ$： $(a,\ b) \longrightarrow a + 2b = a \circ b$

适合不适合结合律？

解 读者可以用解上一题的方法来证明，所给代数运算不适合结合律．

3． $A = \{a,\ b,\ c\}$．由表

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

给出的代数运算适合不适合结合律？

解 所给代数运算$\circ$适合结合律。为了得出这个结论，需要对元素a，b，c的27（$=3^3$）种排列（元素允许重复出现）加以验证。但是利用元素a的特性，可以把验证简化。仔细考察运算表，我们发现以下规律：对集合A的任意元素x来说，都有

$$a\circ x=x\circ a=x$$

由此得出，对于有a出现的排列，结合律都成立。这一点读者可以自己验证。还剩下a不出现的排列。这样的排列共有8（$=2^3$）种。我们在这里验证4种，其余4种读者可以自己验证。

$$(b\circ b)\circ b=c\circ b=a$$
$$b\circ(b\circ b)=b\circ c=a$$

所以 $$(b\circ b)\circ b=b\circ(b\circ b)$$

$$(b\circ b)\circ c=c\circ c=b$$
$$b\circ(b\circ c)=b\circ a=b$$

所以 $$(b\circ b)\circ c=b\circ(b\circ c)$$

$$(b\circ c)\circ b=a\circ b=b$$
$$b\circ(c\circ b)=b\circ a=b$$

所以 $$(b\circ c)\circ b=b\circ(c\circ b)$$

$$(b\circ c)\circ c=a\circ c=c$$
$$b\circ(c\circ c)=b\circ b=c$$

所以 $$(b\circ c)\circ c=b\circ(c\circ c)$$

§5. 交换律

1. $A=$\{所有实数\}，$\circ$是普通减法：

$$a \circ b = a - b$$

这个代数运算适合不适合交换律？

解 容易验证，当 $a=1$，$b=2$ 时

$$a \circ b \neq b \circ a$$

所以这个代数运算不适合交换律。

2. $A=\{a, b, c, d\}$。由表

	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	b	d
d	d	c	a	b

所给的代数运算适合不适合交换律？

解 要回答这个问题，只须考察一下运算表，看一看关于主对角线对称的位置上，有没有不相同的元素。

§6. 分配律

假定$\odot$，$\oplus$是A的两个代数运算，并且$\oplus$适合结合律，$\odot$，$\oplus$适合两个分配律。证明

$$\begin{aligned}&(a_1\odot b_1)\oplus(a_1\odot b_2)\oplus(a_2\odot b_1)\oplus(a_2\odot b_2)\\=&(a_1\odot b_1)\oplus(a_2\odot b_1)\oplus(a_1\odot b_2)\oplus(a_2\odot b_2)\end{aligned}$$

解 $(a_1\odot b_1)\oplus(a_1\odot b_2)\oplus(a_2\odot b_1)\oplus(a_2\odot b_2)$

$$\begin{aligned}&=a_1\odot(b_1\oplus b_2)+a_2\odot(b_1\oplus b_2)\\&=(a_1\oplus a_2)\odot(b_1\oplus b_2)\\&=(a_1\oplus a_2)\odot b_1\oplus(a_1\oplus a_2)\odot b_2\\&=(a_1\odot b_1)\oplus(a_2\odot b_1)\oplus(a_1\odot b_2)\oplus(a_2\odot b_2)\end{aligned}$$

§ 7． 一一映射、变换

1． $A=\{$所有>0的实数$\}$．$\overline{A}=\{$所有实数$\}$．找一个A与$\overline{A}$间的一一映射．

解 Φ： $x\longrightarrow \lg x$ 对一切$x\in A$

是一个A与$\overline{A}$间的一一映射．

首先，给了任一$x\in A$，即任一大于0的实数x，$\lg x$是一个实数，即$\lg x\in\overline{A}$，并且$\lg x$是唯一确定的，所以Φ是一个A到$\overline{A}$的映射．

其次，对于任一$y\in\overline{A}$，即任一实数y，$10^{y}=x$是一个大于0的实数，而在Φ之下，

$$x\longrightarrow \lg x=\lg 10^{y}=y$$

所以Φ是一个A到$\overline{A}$的满射．

最后，若是x_1，$x_2\in A$，并且$x_1\neq x_1$，那么$\lg x_1\neq \lg x_2$，所以Φ是一个A到$\overline{A}$的单射．

这样，Φ是一个A与$\overline{A}$间的一一映射．

2． $A=\{$所有≥ 0的实数$\}$

$\overline{A}=\{$所有实数$\overline{a}$，$0\leq\overline{a}\leq 1$ $\}$

找一个A到$\overline{A}$的满射．

解 Φ： $x\longrightarrow x$ 若$0\leq x<1$

$$x\longrightarrow \frac{1}{x} \quad 若 x\geq 1$$

是一个A到$\overline{A}$的满射．

首先，Φ替每一$x\in A$规定了一个唯一确定的象$\Phi(x)$，

而 $0\leq\Phi(x)\leq 1$，所以Φ是一个A到$\overline{A}$的映射。其次，在Φ之下，$\overline{A}$的每一元$\overline{a}$都是A中一个元，即$\overline{a}$本身的象，所以Φ是一个A到$\overline{A}$的满射。

读者可以证明：

Φ_1: $\quad x\longrightarrow|\sin x| \qquad x\in A$

Φ_2: $\quad x\longrightarrow 0 \qquad 0\leq x<1$

$$x\longrightarrow\frac{1}{x} \qquad x\geq 1$$

都是A到$\overline{A}$的满射。

3. 假定Φ是A与$\overline{A}$间的一个一一映射，a是A的一个元。

$$\Phi^{-1}[\Phi(a)]=? \qquad \Phi[\Phi^{-1}(a)]=?$$

若Φ是A的一个一一变换，这两个问题的回答又该是什么？

解 当Φ是A与$\overline{A}$间的一个一一映射时，

$\Phi^{-1}[\Phi(a)]=a \qquad \Phi[\Phi^{-1}(a)]$未必有意义。

若Φ是A的一个一一变换，那么

$$\Phi^{-1}[\Phi(a)]=a \qquad \Phi[\Phi^{-1}(a)=a$$

读者可以做一做以下补充习题。

(i) $\quad A=\{$所有≥ 0的整数$\}$

$\overline{A}=\{$所有>0的整数$\}$

证明

Φ: $\quad x\longrightarrow x+1 \qquad$ 对一切$x\in A$

是A与$\overline{A}$间的一个一一映射。

(ii) $\quad A=\{$所有≥ 0的实数$\}$

$\overline{A}$ = { 所有 >0 的实数 }

利用（i）题找一个 A 与 $\overline{A}$ 间的一一映射。

§8. 同　态

1. A = { 所有实数 x }. A 的代数运算是普通乘法。以下映射是不是 A 到 A 的一个子集 $\overline{A}$ 的同态满射？

a) $x \to |x|$　　b) $x \to 2x$　　c) $x \to x^2$

d) $x \to -x$

解　a)　取 $\overline{A}$ = { 所有 ≥ 0 的实数 }，则 $\overline{A} \subset A$，而

Φ_1:　　$x \to |x| = \Phi_1(x)$　　$x \in A$

是 A 到 $\overline{A}$ 的一个同态满射。因为：对任一实数 x，$|x|$ 是一个唯一确定的 ≥ 0 的实数，所以 Φ_1 是 A 到 $\overline{A}$ 的一个映射；若是 $\bar{x} \in \overline{A}$，那么 $\bar{x} \in A$，

而

$$\Phi_1(\bar{x}) = |\bar{x}| = \bar{x}$$

所以 Φ_1 是 A 到 $\overline{A}$ 的一个满射；对任意 x，$y \in A$，

$$\Phi_1(xy) = |xy| = |x||y| = \Phi_1(x)\Phi_1(y)$$

所以 Φ_1 是 A 到 $\overline{A}$ 的一个同态满射。

b)　当 x 取遍一切实数值时，$2x$ 也取遍一切实数值。读者容易证明

Φ_2:　　$x \to 2x = \Phi_2(x)$

是 A 到 A 的一个满射，但 Φ_2 不是 A 到 A 的一个同态满射。因为：取 A 的数 2 和 3，那么

$$\Phi_2(2) = 4 \qquad \Phi_2(3) = 6$$

$$\Phi_2\ (2.3)=\Phi_2(6)=12\neq\Phi_2(2)\ \Phi_2(3)$$

c）取$\overline{A}=\{$所有≥ 0的实数$\}$，那么$\overline{A}\subset A$。读者可以自己证明

$$\Phi_3:\qquad x\to x^2=\Phi_3(x)\qquad x\in A$$

是A到$\overline{A}$的一个同态满射。

d）　当x取遍一切实数值时，$-x$也取遍一切实数值。容易证明

$$\Phi_4:\qquad x\to -x=\Phi_4(x)\qquad x\in A$$

是A到A的一个满射，但不是一个同态满射。

2． 假定A和$\overline{A}$对于代数运算$\circ$和$\bar{\circ}$来说同态，而$\overline{A}$和$\overline{\overline{A}}$对于代数运算$\bar{\circ}$和$\bar{\bar{\circ}}$来说同态。证明，A和$\overline{\overline{A}}$对于代数运算$\circ$和$\bar{\bar{\circ}}$说同态。

解　由题设存在A到$\overline{A}$的一个同态满射

$$\Phi_1:\qquad a\to\bar{a}=\Phi_1(a)\qquad a\in A,\ \bar{a}\in\overline{A}$$

并且对于A的任意两个元素a和b来说

$$\Phi_1\ (a\circ b)\ =\bar{a}\ \bar{\circ}\ \bar{b}=\Phi_1(a)\ \bar{\circ}\ \Phi_1(b)$$

同样存在$\overline{A}$到$\overline{\overline{A}}$的一个同态满射

$$\Phi_2:\qquad \bar{a}\to\bar{\bar{a}}=\Phi_2\ (\bar{a})\qquad \bar{a}\in\overline{A},\ \bar{\bar{a}}\in\overline{\overline{A}}$$

并且对于$\overline{A}$的任意两个元素$\bar{a}$和$\bar{b}$来说

$$\Phi_2\ (\bar{a}\ \bar{\circ}\ \bar{b})\ =\bar{\bar{a}}\ \bar{\bar{\circ}}\ \bar{\bar{b}}=\Phi_2\ (\bar{a})\ \bar{\bar{\circ}}\ \Phi_2\ (\bar{b})$$

如下定义

$$\Phi:\qquad a\to\Phi_2[\Phi_1(a)]\qquad a\in A$$

那么Φ是A到$\overline{\overline{A}}$的一个同态满射。因为：

（i）　由于Φ_1和Φ_2是同态满射，所以对于任何$a\in A$，$\Phi_1(a)$是$\overline{A}$的一个唯一确定的元素，而$\Phi_2[\Phi_1(a)]$是$\overline{\overline{A}}$的一个唯一确定的元素，因而Φ是A到$\overline{\overline{A}}$的一个映射。

(ii) 由于同一原因，对于任何$\bar{\bar{a}} \in \bar{\bar{A}}$，存在一个元素$\bar{a} \in \bar{A}$，使$\Phi_2(\bar{a}) = \bar{\bar{a}}$，并且存在一个元素$a \in A$，使$\Phi_1(a) = \bar{a}$，因此在$\Phi$之下，

$$a \to \Phi_2[\Phi_1(a)] = \Phi_2(\bar{a}) = \bar{\bar{a}}$$

而Φ是A到$\bar{\bar{A}}$的一个满射。

(iii) 由于同一原因，对于A的任何两个元素a和b

$$\begin{aligned}\Phi(a \circ b) &= \Phi_2[\Phi_1(a \circ b)] = \Phi_2[\Phi_1(a) \bar{\circ} \Phi_1(b)] \\ &= \Phi_2[\Phi_1(a)] \bar{\bar{\circ}} \Phi_2[\Phi_1(b)] \\ &= \Phi(a) \bar{\bar{\circ}} \Phi(b)\end{aligned}$$

而Φ是A到$\bar{\bar{A}}$的一个同态满射。

§ 9. 同构、自同构

1. $A = \{a, b, c\}$。代数运算$\circ$由下表给定：

	a	b	c
a	c	c	c
b	c	c	c
c	c	c	c

找出所有A的一一变换，对于代数运算$\circ$来说，这些一一变换是否都是A的自同构？

解 A共有$6(=3!)$个一一变换，即

Φ_1: $a \to a$ $b \to b$ $c \to c$

Φ_2: $a \to a$ $b \to c$ $c \to b$

Φ_3: $a \to b$ $b \to c$ $c \to a$

Φ_4:　　　$a \to b$　　$b \to a$　　$c \to c$

Φ_5:　　　$a \to c$　　$b \to b$　　$c \to a$

Φ_6:　　　$a \to c$　　$b \to a$　　$c \to b$

对于代数运算 o 来说，Φ_1 和 Φ_4 是 A 的自同构，其余 4 个都不是。这是因为，若 Φ_i 是一个 A 的自同构，那么对 A 的任何元素 x 和 y，将有

(1)　　$\Phi_i(x o y) = \Phi_i(c) = \Phi_i(x) o \Phi_i(y) = c$

因而

(2)　　$\Phi_i(c) = c$

反过来，若（2）成立，那么（1）也成立。

2. $A = \{$所有有理数$\}$。找一个 A 的对于普通加法来说的自同构。（映射 $x \to x$ 除外）。

解　设 k 是任一有理数，且 $k \neq 0$，$k \neq 1$。

那么

Φ:　　$x \to kx$　　$x \in A$

是 A 的一个对于加法来说的自同构，并且 Φ 显然不是映射 $x \to x$。Φ 是 A 的一个一一变换，读者可以自己证明。令 x 和 y 是 A 的任意两个元素，那么

Φ:　$x + y \to \Phi(x+y) = k(x+y) = kx + ky = \Phi(x) + \Phi(y)$

所以 Φ 是 A 的一个自同构。

读者可以试证，A 只有以下对于加法来说的自同构

$x \to kx$　　$x \in A$，k 是 $\neq 0$ 的有理数

3. $A = \{$所有有理数$\}$；A 的代数运算是普通加法。$\overline{A} = \{$所有 $\neq 0$ 的有理数$\}$；$\overline{A}$ 的代数运算是普通乘法。证明，对于给的代数运算来说，A 与 $\overline{A}$ 间没有同构映射存在。（先决定 0 在一个同构映射下的象。）

解 设Φ是A与$\overline{A}$间对于所给代数运算的一个同构映射，而$\Phi(0)=\overline{a}$。那么由于Φ是同构映射，有

$$\Phi(0)=\Phi(0+0)=\Phi(0)\Phi(0)=\overline{a}^2$$

但同构映射是单射，所以得$\overline{a}=\overline{a}^2$。于是有

$$\overline{a}^2-\overline{a}=\overline{a}(\overline{a}-1)=0$$

但$\overline{a}\in\overline{A}$，所以$\overline{a}\neq 0$，因而$\overline{a}-1=0$，即$\overline{a}=1$。这样

$$\Phi(0)=1 \qquad (1)$$

由于Φ是满射，$\overline{A}$的元-1必是A的某一元a的象：

$$\Phi(a)=-1$$

由是得

$$\Phi(2a)=\Phi(a+a)=\Phi(a)\Phi(a)=(-1)^2=1$$

于是由Φ是单射，得$2a=0$，即$a=0$，而$\Phi(0)=-1$，与（1）矛盾。这说明，在A与$\overline{A}$间对所给代数运算来说不存在同构对应。

读者可以用以下方法得出本题的另一证明：

设$\Phi(a)=2$。考虑$\Phi\left(\frac{a}{2}+\frac{a}{2}\right)$

§10. 等价关系与集合的分类

1. $A=\{$所有实数$\}$。A的元间的关系$>$以及$\geq$是不是等价关系？

解 $>$不是等价关系。这个关系不满足反射律：$a>a$不成立。

$\geq$也不是等价关系，它不满足对称律，例如，$3\geq 2$，但$2\geq 3$不成立。

2． 有人说：假如一个关系R适合对称律和推移律，那么它也适合反射律。他的推论方法是：因为R适合对称律

$$a\,R\,b \Longrightarrow b\,R\,a$$

因为R适合推移律

$$a\,R\,b,\quad b\,R\,a \Longrightarrow a\,R\,a$$

这个推论方法有什么错误？

解 这个推论方法的错误在于，对于“等价关系”定义的陈述没有准确地理解。

$$a\,R\,b \Longrightarrow b\,R\,a$$

的意思是：由$a\,R\,b$可得$b\,R\,a$；假如对于某一元素a，找不到任何元素b，使得$a\,R\,b$成立，那么就得不出$b\,R\,a$，因而也就得不出$a\,R\,a$。例如：令A是整数集，如下定义A的元间的关系R：

$$a\,R\,b \quad \text{当且仅当}\ ab>0.$$

R显然满足对称律和推移律，但R不满足反射律，因为

$$0\,R\,0$$

不成立。

3． 仿照例3规定整数间的关系

$$a\equiv b \quad (-5)$$

证明你所规定的是一个等价关系，并且找出模－5的剩余类。

解 可以完全仿照例3来做。

第二章　群论

§1.　群的定义

1.　全体整数的集合对于普通减法来说是不是一个群？

解　不是，因为普通减法不适合结合律。

例如

$$3-(2-1)=3-1=2 \qquad (3-2)-1=1-1=0$$

$$3-(2-1)\neq(3-2)-1$$

2.　举一个有两个元的群的例。

解　令$G=\{e, a\}$，G的乘法由下表给出

	e	a
e	e	a
a	a	e

首先，容易验证，这个代数运算满足结合律

(1)　　$(xy)z=x(yz)$　　$x, y, z\in G$

因为，由于$ea=ae=a$，若是元素e在（1）中出现，那么（1）成立。（参考第一章，§4，习题3.）若是e不在（1）中出现，那么有

$$(aa)a=ea=a \qquad a(aa)=ae=a$$

而（1）仍成立。

其次，G有左单位元，就是e；e有左逆元，就是e，a有左逆元，就是a。所以G是一个群。

读者可以考虑一下，以上运算表是如何作出的。

3． 证明，我们也可以用条件Ⅰ，Ⅱ以及下面的条件Ⅳ′，Ⅴ′来做群的定义：

Ⅳ′ G里至少存在一个右逆元a^{-1}，能让

$$ae = a$$

对于G的任何元a都成立；

Ⅴ′ 对于G的每一个元a，在G里至少存在一个右逆元a^{-1}，能让

$$aa^{-1} = e$$

解 这个题的证法完全平行于本节中关于可以用条件Ⅰ，Ⅱ，Ⅳ，Ⅴ来做群定义的证明，但读者一定要自己写一下。

§2. 单位元、逆元、消去律

1． 若群G的每一个元都适合方程$x^2=e$，那么G是交换群。

解 令a和b是G的任意两个元。由题设

$$(ab)(ab) = (ab)^2 = e$$

另一方面

$$(ab)(ba) = ab^2a = aea = a^2 = e$$

于是有 $(ab)(ab) = (ab)(ba)$。利用消去律，得

$$ab = ba$$

所以G是交换群。

2. 在一个有限群里，阶大于2的元的个数一定是偶数。

解 令G是一个有限群。设G有元a而a的阶$n>2$。考察a^{-1}。我们有

$$a^n(a^{-1})^n=e \qquad e(a^{-1})^n=(a^{-1})^n=e$$

设正整数$m<n$而$(a^{-1})^m=e$，那么同上可得$a^m=e$，与n是a的阶的假设矛盾。这样，n也是a^{-1}的阶，易见$a^{-1}\neq a$。否则

$$a^2=aa^{-1}=e$$

与$n>2$的假设矛盾。这样，我们就有一对不同的阶大于2的元a和a^{-1}。

设G还有元b，$b\neq a$，$b\neq a^{-1}$，并且b的阶大于2。那么b^{-1}的阶也大于2，并且$b^{-1}\neq b$。我们也有$b^{-1}\neq a$。否则

$$e=b^{-1}b=aa^{-1}=b^{-1}a^{-1}$$

消去b^{-1}得$b=a^{-1}$，与假设矛盾。同样可证$b^{-1}\neq a^{-1}$。这样，除a和a^{-1}外，又有一对不同的阶大于2的元b和b^{-1}。

由于G是有限群，而G的阶大于2的元总是成对出现，所以G里这种元的个数一定是偶数。

3. 假定G是一个阶是偶数的有限群。在G里阶等于2的元的个数一定是奇数。

解 由习题2知，G里阶大于2的元的个数是偶数。但G只有一个阶是1的元，就是单位元e。于是由于G的阶是偶数，得G里阶等于2的元的个数是奇数。

4. 一个有限群的每一个元的阶都有限。

解 令G是一个有限群而a是G的任一元素，那么

$$a, \ a^2, \ a^3, \ \cdots$$

不能都不相等。因此存在正整数 i，j，$i>j$，使 $a^i=a^j$。用 a^{-j} 乘两边，得

$$(1) \qquad a^{i-j}=e$$

这样，存在正整数 $i-j$，使（1）成立。因此也存在最小的正整数 m，使 $a^m=e$，这就是说，元 a 的阶是 m。

§4. 群的同态

假定在两个群 G 和 $\bar{G}$ 的一个同态映射之下，$a\to\bar{a}$。a 与 $\bar{a}$ 的阶是不是一定相同？

解 不一定。例如，令 G 是本章§1中例2所给出的群而 $\bar{G}$ 是该节中例1所给出的群。那么读者容易证明

$$\Phi: \qquad n\to g \qquad n \text{ 是 } G \text{ 的任意元}$$

是 G 到 $\bar{G}$ 的一个同态映射。但 G 的每一个元 $n\neq 0$ 都是无限阶的，而 g 的阶是1。

§5. 变换群

1. 假定 τ 是集合 A 的一个非一一变换。τ 会不会有一个左逆元 τ^{-1} 使得 $\tau^{-1}\tau=\varepsilon$？

解 可能有。例如令 $A=\{$所有正整数$\}$，则

$$\tau: \qquad 1\to 1, \qquad n\to n-1 \qquad n>1$$

显然是 A 的一个非一一变换。而 A 的变换

$$\tau^{-1}: \qquad n\to n+1 \qquad n\in A$$

就能使 $\tau^{-1}\tau=\varepsilon$。

2. 假定A是所有实数作成的集合。证明，所有A的可以写成

$$x \to ax+b \qquad a\text{和}b\text{是有理数，}a\neq 0$$

形式的变换作成一个变换群。这个群是不是一个交换群？

解 令G是由一切上述变换作成的集合。考察G的任何两个元素

τ： $\quad x\to ax+b \qquad a$和b是有理数，$a\neq 0$

λ： $\quad x\to cx+d \qquad c$和d是有理数，$c\neq 0$

那么

$\tau\lambda$： $\quad x\to x^{\tau\lambda}=(ax+b)^{\lambda}=c(ax+b)+d$

$$=(ca)x+(cb+d)$$

这里ca和$cb+d$都是有理数，并且$ca\neq 0$。

所以$\tau\lambda$仍属于G。

结合律对一般变换都成立，所以对上述变换也成立。

单位变换

ε： $\quad x\to x$

属于G。

容易验证，τ在G中有逆，即

τ^{-1}： $\quad x\to \frac{1}{a}x+\left(-\frac{b}{a}\right)$

因此G作成一个变换群。

但G不是一个交换群。令

τ_1： $\quad x\to x+1$

τ_2： $\quad x\to 2x$

那么

$\tau_1\tau_2$： $\quad x\to (x^{\tau_1})^{\tau_2}=(x+1)^{\tau_2}=2x+2$

$\tau_2\tau_1$: $\qquad x \to (x^{\tau_2})^{\tau_1} = (2x)^{\tau_1} = 2x+1$

$$\tau_1\tau_2 \neq \tau_2\tau_1$$

3. 假定S是一个集合A的所有变换作成的集合。我们暂时仍用符号

τ: $\qquad a \longrightarrow a' = \tau(a)$

来说明一个变换τ。证明，我们可以用

$\tau_1\tau_2$: $\qquad a \longrightarrow \tau_1[\tau_2(a)] = \tau_1\tau_2(a)$

来规定一个S的乘法，这个乘法也适合结合律并且对于这个乘法来说，ε还是S的单位元。

解 令τ_1和τ_2是S的任意两个元而a是A的任意一个元。那么$\tau_2(a)$和$\tau_1[\tau_2(a)]$都是A的唯一确定的元。因此如上规定的$\tau_1\tau_2$仍是S的一个唯一确定的元而我们得到了一个S的乘法。

令τ_3也是S的一个任意元，那么

$$[(\tau_1\tau_2)\tau_3](a) = \tau_1\tau_2[\tau_3(a)] = \tau_1\{\tau_2[\tau_3(a)]\}$$

$$[\tau_1(\tau_2\tau_3)](a) = \tau_1[\tau_2\tau_3(a)] = \tau_1\{\tau_2[\tau_3(a)]\}$$

所以 $(\tau_1\tau_2)\tau_3 = \tau_1(\tau_2\tau_3)$ 而乘法适合结合律。

令τ是S的任意元。由于对一切$a \in A$，都有$\varepsilon(a) = a$，所以

$$\varepsilon\tau(a) = \varepsilon[\tau(a)] = \tau(a)$$

$$\tau\varepsilon(a) = \tau[\varepsilon(a)] = \tau(a)$$

即$\varepsilon\tau = \tau\varepsilon = \tau$而$\varepsilon$仍是$S$的单位元。

4. 证明，一个变换群的单位元一定是恒等变换。

解 设G是由某一集合A的变换组成的一个变换群，而ε是G的单位元。任取G的一个元τ和A的一个元a。由于

$\varepsilon\tau=\tau$，有

$$a^{\varepsilon\tau}=(a^{\varepsilon})^{\tau}=a^{\tau}$$

由于τ是A的一个一一变换，所以$a^{\varepsilon}=a$而ε是A的恒等变换。

5． 证明，实数域上一切有逆的$n\times n$矩阵对于矩阵乘法来说，作成一个群。

解 这个题的解法很容易，这里从略。

§6． 置换群

1． 找出所有S_3的不能和$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$交换的元。

解 S_3有6个元：

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

其中的

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^2$$

显然可以和$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ 交换．通过计算，易见其它三个元不能和$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$交换。

2． 把S_3的所有元写成不相连的循环置换的乘积。

解 $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=(1)$，$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(2\ 3)$

$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(1\ 2)$，$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(1\ 3)$，$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1\ 2\ 3)$

$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(1\ 3\ 2)$

3. 证明：

（i）两个不相连的循环置换可以交换；

（ii）$(i_1 i_2 \cdots i_k)^{-1} = (i_k i_{k-1} \cdots i_1)$。

解 （i）看S_n的两个不相连的循环置换σ和τ。我们考察乘积$\sigma\tau$使数字1，2，…，n如何变动。有三种情况。

（a） 数字i在σ中出现，并且σ把i变成j。这时由于σ和τ不相连，j不在τ中出现，因而τ使j不变，所以$\sigma\tau$仍把i变成j。

（b） 数字k在τ中出现，并且τ把k变成l。这时k不在σ中出现，因而σ使k不变，所以$\sigma\tau$仍把k变成l。

（c）数字m不在σ和τ中出现。这时$\sigma\tau$使m不动。

如上考察$\tau\sigma$使数字1，2，…，n如何变动，显然得到同样的结果。因此$\sigma\tau = \tau\sigma$。

（ii） 由于$(i_1 i_2 \cdots i_k)(i_k i_{k-1} \cdots i_1) = (1)$，所以

$$(i_1 i_2 \cdots i_k)^{-1} = (i_k i_{k-1} \cdots i_1)$$

4. 证明一个k－循环置换的阶是k。

解 一个k－循环置换$\pi = (i_1 i_2 \cdots i_k)$的一次方，二次方，…，$k$次方分别把$i_1$变成$i_2$，$i_3$，…，$i_1$。同理$\pi^k$把$i_2$变成$i_2$，…，把$i_k$变成$i_k$。因此$\pi^k = (1)$。由上面的分析，若是$l < k$，那么$\pi^l \neq (1)$。这就证明了，$\pi$的阶是$k$。

5. 证明S_n的每一个元都可以写成

$$(1\ 2),\ (1\ 3),\ \cdots,\ (1\ n)$$

这$n-1$个2－循环置换中的若干个的乘积。

解 由于每一个置换都可以写成不相连的循环置换的乘积，所以只须证明，一个循环置换可以写成若干个$(1\ i)$形的置换的乘积。设π是一个k－循环置换。我们分两个情形

加以讨论。

(a) 1在π中出现，这时π可以写成

$$(1\, i_1 i_2 \cdots i_{k-1})$$

容易验算

$$(1\, i_1 i_2 \cdots i_{k-1}) = (1\, i_1)(1\, i_2)\cdots(1\, i_{k-1})$$

(b) 1不在π中出现，这时

$$\pi = (i_1 i_2 \cdots i_k) = (1\, i_1 i_2 \cdots i_k)(1\, i_1)$$
$$= (1\, i_1)(1\, i_2)\cdots(1\, i_k)(1\, i_1)$$

§7. 循环群

1. 证明，一个循环群一定是交换群。

解 设循环群$G=(a)$。那么G的任何两个元都可以写成a^m和a^n(m，n是整数）的形式。但

$$a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$$

所以G是一个交换群。

2. 假定群的元a的阶是n。证明a^r的阶是$\frac{n}{d}$，这里$d=(r,n)$是r和n的最大公因子。

解 由于$d \mid r$，$r=ds$，所以

$$(a^r)^{\frac{n}{d}} = (a^{ds})^{\frac{n}{d}} = (a^n)^s = e$$

现在证明，$\frac{n}{d}$就是a^r的阶。设a^r的阶为k。那么$k \leq \frac{n}{d}$。令

$$\frac{n}{d} = kq + r_1 \qquad 0 \leq r_1 \leq k-1$$

得

$$e=(a^r)^{\frac{n}{d}}=(a^r)^{kq+r_1}=(a^r)^{kq}(a^r)^{r_1}=(a^r)^{r_1}$$

但$r_1<k$而k是a^r的阶，所以$r_1=0$而

$$\frac{n}{d}=kq$$

于是得$k\left|\frac{n}{d}\right.$。（参看本节定理的第二种情形。）

为了证明$k=\frac{n}{d}$，只须反过来证明$\frac{n}{d}\left|k\right.$。由$a^{rk}=e$而$n$是$a$的阶，同上有$n|rk$，因而$\frac{n}{d}\left|\frac{r}{d}k\right.$。但$d$是$n$和$r$的最大公因子，所以$\frac{n}{d}$和$\frac{r}{d}$互素而有$\frac{n}{d}\left|k\right.$。

3． 假定a生成一个阶是n的循环群G。证明：a^r也生成G，假如$(r, n)=1$（这就是说r和n互素）。

解 由习题2，a^r的阶是n。所以

$$a^r,\ (a^r)^2,\ \cdots,\ (a^r)^{n-1},\ (a^r)^n=e$$

互不相同。但G只有n个元，所以

$$G=\{a^r,\ (a^r)^2,\ \cdots,\ (a^r)^n\}$$

而a^r生成G。

4． 假定G是循环群，并且G与$\bar{G}$同态。证明$\bar{G}$也是循环群。

解 由于G与$\bar{G}$同态，$\bar{G}$也是一个群。设$G=(a)$，而在G到$\bar{G}$的同态满射Φ下，$a\longrightarrow\bar{a}$。看$\bar{G}$的任意元$\bar{g}$。那么在Φ下，有$a^m\in G$，使$a^m\longrightarrow\bar{g}$。但$a^m\longrightarrow\bar{a}^m$。所以$\bar{g}=\bar{a}^m$。

这样，$\bar{G}$的每一元都是$\bar{a}$的一个乘方而$\bar{G}=(\bar{a})$。

5. 假定G是无限阶的循环群，$\bar{G}$是任何循环群。证明G与$\bar{G}$同态。

解 令$G=(a)$，$\bar{G}=(\bar{a})$。定义

$$\Phi: \qquad a^m \longrightarrow \bar{a}^m$$

我们证明，Φ是G到$\bar{G}$的一个同态满射。

(i) 由于G是无限阶的循环群，G的任何元都只能以一种方法写成a^m的形式，所以在Φ之下，G的每一个元有一个唯一确定的象，而Φ是G到$\bar{G}$的一个映射。

(ii) $\bar{G}$的每一个元都可以写成$\bar{a}^m$的形式，因此它在Φ之下是G的元a^m的象，而Φ是G到$\bar{G}$的一个满射。

(iii) $$a^m a^n = a^{m+n} \longrightarrow \bar{a}^{m+n} = \bar{a}^m \bar{a}^n$$

所以Φ是G到$\bar{G}$的一个同态满射。

§8. 子　　群

1. 找出S_3的所有子群。

解 S_3显然有以下子群：

S_3本身；$((1))=\{(1)\}$；

$((1\ 2))=\{(1\ 2),\ (1)\}$；

$((1\ 3))=\{(1\ 3),\ (1)\}$；

$((2\ 3))=\{(2\ 3),\ (1)\}$；

$((1\ 2\ 3))=\{(1\ 2\ 3),\ (1\ 3\ 2),\ (1)\}$。

若S_3的一个子群H含有$(1\ 2)$，$(1\ 3)$这两个2－循环置换，那么H含有

$$(1\ 2)(1\ 3)=(1\ 2\ 3),\ (1\ 2\ 3)(1\ 2)=(2\ 3)$$

因而$H=S_3$。同理，若是S_3的一个子群含有两个2-循环置换$(2\ 1)$，$(2\ 3)$或$(3\ 1)$，$(3\ 2)$，这个子群也必然是S_3。

用完全类似的方法，读者可以算出，若是S_3的一个子群含有一个2-循环置换和一个3-循环置换，那么这个子群也必然是S_3。

因此上面给出的6个子群是S_3的所有子群。

2． 证明，群G的两个子群的交集也是G的子群。

解 设H_1和H_2是G的子群。

令e是G的单位元。那么e属于H_1和H_2，因而

$$e\in H_1\cap H_2$$

而$H_1\cap H_2$不空。

令a，$b\in H_1\cap H_2$。那么a，b属于H_1和H_2。但H_1和H_2是子群。所以ab^{-1}属于H_1和H_2，因而属于$H_1\cap H_2$。

这就证明了，$H_1\cap H_2$是G的子群。

3． 取S_3的子集$S=\{(1\ 2),(1\ 2\ 3)\}$。S生成的子群包含哪些元？一个群的两个不同的子集会不会生成相同的子群？

解 见习题1的解。

4． 证明，循环群的子群也是循环群。

解 设循环群$G=(a)$而H是G的一个子群。

若H只含单位元$e=a^0$，则$H=(e)$是循环群。若H不仅含单位元，那么因为H是子群，它一定含有元a^m，其中m是正整数。令i是最小的使得a^i属于H的正整数，我们证明，这时$H=(a^i)$。看H的任一元a^t。令

$$t = iq + r \qquad 0 \leq r < i$$

那么 $a^t = a^{iq}a^r$。由于 a^t 和 a^{iq} 都属于H，有

$$a^r = a^{-iq}a^t \in H$$

于是由假设 $r = 0$，$a^t = (a^i)^q$ 而$H = (a^i)$。

5. 找出模12的剩余类加群的所有子群。

解 模12的剩余类加群G是一个阶为12的循环群。因此由题 4，G的子群都是循环群。容易看出：

([0]) = [0]

([1]) = ([5]) = ([7]) = ([11]) = G

([2]) = ([10]) = {[2], [4], [6], [8], [10], [0]}

([3]) = ([9]) = {[3], [6], [9], [0]}

([4]) = ([8]) = {[4], [8], [0]}

([6]) = {[6], [0]}

是G的所有子群。

6. 假定H是群G的一个非空子集并且H的每一个元的阶都有限。证明，H作成一个子群的充要条件是：

$$a,\ b \in H \Longrightarrow ab \in H$$

解 由本节定理 1，条件显然是必要的。

要证明条件也是充分的，由同一定理，只须证明：

$$a \in H \Longrightarrow a^{-1} \in H$$

设 $a \in H$。由于H的每一元的阶都有限，所以 a 的阶是某一正整数 n 而$a^{-1} = a^{n-1}$。于是由所给条件得 $a^{-1} \in H$。

§9. 子群的陪集

1. 证明，阶是素数的群一定是循环群。

解　设群G的阶为素数p。在G中取一元$a \neq e$，则a生成G的一个循环子群(a)。设(a)的阶为n，那么$n \neq 1$。但由定理2，$n \mid p$，所以$n = p$而$G = (a)$是一个循环群。

2. 证明，阶是p^m的群（p是素数，$m \geq 1$）一定包含一个阶是p的子群。

解　设群G的阶是p^m。在G中取一元$a \neq e$，那么由定理3，a的阶$n \mid p^m$。但$n \neq 1$，所以$n = p^t$，$t \geq 1$。若$t = 1$，那么a的阶为p，而(a)是一个阶为p的子群。若$t > 1$，可取$b = a^{p^{t-1}}$，那么b的阶为p而(b)是一个阶为p的子群。

3. 假定a和b是一个群G的两个元，并且$ab = ba$，又假定a的阶是m，b的阶是n，并且$(m, n) = 1$。证明：ab的阶是mn。

解　设ab的阶是k。由$ab = ba$，得

$$(ab)^{mn} = a^{mn}b^{mn} = e$$

因此$k \mid mn$。我们反过来证明，$mn \mid k$。由

$$e = (ab)^{kn} = a^{kn}b^{kn} = a^{kn}$$

以及a的阶为m，得$m \mid kn$。但$(m, n) = 1$，所以$m \mid k$。同理$n \mid k$。又由$(m, n) = 1$，得$mn \mid k$。

这样，ab的阶$k = mn$。

4. 假定$\sim$是一个群G的元间的一个等价关系，并且对于G的任意三个元a，x，x'来说

$$ax \sim ax' \Longrightarrow x \sim x'$$

证明，与G的单位元e等价的元所作成的集合是G的一个子群。

解　令H是与e等价的元所成的集合。

由于 $e\sim e$，所以H不空。

设 a，$b\in H$。那么 $a\sim e$， $b\sim e$。$b\sim e$ 可写成

$$a^{-1}ab\sim a^{-1}a$$

因此由题设，$ab\sim a\sim e$ 而 $ab\in H$。

$a\sim e$ 可写成 $ae\sim aa^{-1}$，因此由题设，$e\sim a^{-1}$ 而 $a^{-1}\in H$。

这样，H 作成 G 的一个子群。

5. 我们直接下右陪集 Ha 的定义如下：Ha 刚好包含 G 的可以写成

$$h\ a \qquad (h\in H)$$

形式的元。由这个定义推出以下事实：G 的每一个元属于而且只属于一个右陪集。

解 取任意元 $a\in G$。由于 H 是一个子群，单位元 $e\in H$，因此 $a=e\ a\in H\ a$，这就是说，元 a 属于右陪集 $H\ a$。

设 $a\in H\ b$， $a\in H\ c$，那么

$$a=h_1b=H_2c \qquad (h_1,\ h_2\in H)$$

由此得，$b=h_1^{-1}h_2\ c$，而 $H\ b$ 的任意元

$$hb=hh_1^{-1}h_2\ c\in H\ c$$

因而 $H\ b\subset H\ c$。同样可证 $H\ c\subset H\ b$。这样 $Hb=Hc$ 而 a 只能属于一个右陪集。

6. 若我们把同构的群看成一样的，一共只存在两个阶是4的群，它们都是交换群。

解 先给出两个阶是4的群。

模4的剩余类加群 $G_1=\{[0],[1],[2],[3]\}$。G_1 的元 $[1]$ 的阶是4而 G_1 是 $[1]$ 所生成的循环群 $([1])$。

S_4的的子群

$$B_4=\{(1),\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (14)(2\,3)\}$$

叫作克莱因四元群. B_4是S_4的子群容易验证. 我们有

$$[(1\,2)(3\,4)]^2=[(1\,3)(2\,4)]^2=[(14)(23)]^2=(1)$$

$$(12)(34)(1\,3)(24)=(13)(24)(12)(3\,4)=(14)(23)$$

$$(13)(24)(14)(23)=(1\,4)(2\,3)(1\,3)(2\,4)=(12)(34)$$

$$(14)(23)(12)(34)=(1\,2)(3\,4)(1\,4)(2\,3)=(13)(24)$$

这两个群显然都是交换群.

现在证明, 任何阶是4的群都和以上两个群之一同构. 设G是一个阶为4的群。那么G的元的阶只能是1, 2或4.

若G有一个阶为4的元d, 那么$G=(d)$是一个循环群而G与G_1同构.

若G没有阶为4的元, 那么除单位元e外, G的其它3个元的阶都是2. 因此有

$$G=\{e,\ a,\ b,\ c\}\qquad a^2=b^2=c^2=e$$

由于G是群, 有$ab\in G$. 我们证明, $ab=c$.

由$ab=e$将得$ab=a^2$和$b=a$, 这不可能.

由$ab=a$将得$b=e$, 也不可能.

由$ab=b$将得$a=e$, 也不可能.

因此只能$ab=c$. 同样可证

$$ab=ba=c,\qquad bc=cb=a,\qquad ca=ac=b$$

比较G和B_4的代数运算, 易见G和B_4同构.

补充题　利用6题证明, 一个有限非交换群至少有6个元。

§10. 不变子群、商群

1. 假定群G的不变子群N的阶是2. 证明，G的中心包含N。

解 令$N=\{e, n\}$，这里e是G的单位元。取G的任意元a。由于N是一个不变子群，有$aN=Na$，即

$$\{a, an\}=\{a, na\}$$

所以$an=na$。这样，N的两个元e和n都可以和G的任何元a交换，所以N属于G的中心。

2. 证明，两个不变子群的交集还是不变子群。

解 令N_1和N_2是群G的两个不变子群. 那么$N_1\cap N_2$，是G的一个子群（§8，习题2）. 我们进一步证明，$N_1\cap N_2$是G的一个不变子群。令$a\in G$，$n\in N_1\cap N_2$，那么$n\in N_1$，$n\in N_2$。但N_1和N_2是不变子群，所以$ana^{-1}\in N_1$，$ana^{-1}\in N_2$，因而

$$ana^{-1}\in N_1\cap N_2$$

于是由定理2，$N_1\cap N_2$是一个不变子群。

3. 证明，指数是2的子群一定是不变子群。

解 令G是一个群而N是G的一个指数为2的子群。

若$n\in N$，那么显然有$nN=Nn$. 设$b\in G$，$b\overline{\in}N$. 那么由于N的指数是2，G被分成两个左陪集N和bN；G也被分成两个右陪集N和Nb. 因此$bN=Nb$. 这样，对于G的任何元a来说，$aN=Na$而N是G的一个不变子群。

4. 假定H是G的子群，N是G的不变子群. 证明，HN是G的子群。

解 由于H和N都不空，所以HN也不空。

设 $a\in HN$，$b\in HN$。那么

$$a=h_1n_1,\quad b=h_2n_2\quad (h_1,\ h_2\in H,\ n_1,\ n_2\in N)$$

$$ab^{-1}=h_1n_1n_2^{-1}h_2^{-1}=h_1n'h_2^{-1}\qquad (n'=n_1n_2^{-1})$$

由于N是一个不变子群，有

$$Nh_2^{-1}=h_2^{-1}N,\quad n'h_2^{-1}=h_2^{-1}n\qquad (n\in N)$$

由是得$ab^{-1}=(h_1h_2^{-1})\,n\in HN$而$HN$是一个子群。

5. 举例证明，G的不变子群N的不变子群N_1未必是G的不变子群（取$G=S_4$）。

解 令$G=S_4$，

$$N=\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

$$N_1=\{(1),\ (12)(34)\}$$

已知N是G的一个子群（上节习题6）。我们证明，N是G的一个不变子群。为了证明这一点，我们考察，是否对一切$\pi\in S_4$，等式

(a) $\qquad \pi N\pi^{-1}=N$

成立。由于任何π都可以写成（$1i$）形的2-循环置换的乘积（§6．习题5），我们只须对（$1i$）形的π来看等式（a）是否成立。又由于N的元的对称性，我们只须看$\pi=(12)$的情形。但

$$(12)\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}(12)$$
$$=\{(1),\ (12)(34),\ (14)(23),\ (13)(24)\}$$

所以N是S_4的一个不变子群。由于N是交换群，N_1当然是N的一个不变子群。但N_1不是S_4的一个不变子群。因为

$(13)[(12)(34)](13)=(14)(23)\in N$;

6. 一个群G的可以写成$a^{-1}b^{-1}ab$形式的元叫作换位子。证明：

(i) 所有有限个换位子的乘积作成的集合C是G的一个不变子群；

(ii) G/C是交换群；

(iii) 若N是G的一个不变子群，并且G/N是交换群，那么

$$N\supset C$$

解 (i) C的两个元的乘积仍是有限个换位子的乘积，因而仍是C的一个元。一个换位子的逆仍是一个换位子，所以C的一个元的逆仍是C的一个元。这样C是一个子群。

对于$a\in G$，$c\in C$，$aca^{-1}=(aca^{-1}c^{-1})c\in C$，所以$C$是$G$的一个不变子群。

(ii) 令a，$b\in G$。那么$a^{-1}b^{-1}ab=c\in C$。由此得

$$ab=bac,\quad abC=bacC=baC$$

即$aCbC=bCaC$而G/C是交换群。

(iii) 因为G/N是交换群，所以对G的任何两个元a和b

$$(aN)(bN)=(bN)(aN),\quad abN=baN$$

由此得 $ab=ban\quad(n\in N)\quad a^{-1}b^{-1}ab=n\in N$。

这样N含有一切换位子，因而含有C。

补充题. 令π和$(i_1i_2\cdots i_k)$属于S_n。证明

$$\pi^{-1}(i_1i_2\cdots i_k)\pi=(i_1^{\pi}\ i_2^{\pi}\ \cdots i_k^{\pi})$$

§11. 同态与不变子群

1. 我们看一个集合A到集合$\overline{A}$的满射Φ。证明，若A的子集S是$\overline{A}$的子集$\overline{S}$的逆象，$\overline{S}$一定是S的象；但若$\overline{S}$是S的象，S不一定是$\overline{S}$的逆象。

解 (i) 设S是$\overline{S}$的逆象。这时对任一元$a\in S$，存在元$\overline{a}\in\overline{S}$，使$\Phi(a)=\overline{a}$，因此$\Phi(S)\subset\overline{S}$。反过来，对任一元$\overline{a}\in\overline{S}$，存在$a\in S$，使$\Phi(a)=\overline{a}$，因此$\overline{S}\subset\Phi(S)$。这样$\overline{S}=\Phi(S)$，即$\overline{S}$是$S$的象。

(ii) 令$A=\{1, 2, 3, 4\}$，$\overline{A}=\{2, 4\}$，A到$\overline{A}$的满射是

Φ: $\quad 1\to 2,\quad 2\to 2,\quad 3\to 4,\quad 4\to 4$

取$S=\{1, 3\}$。那么S的象$\overline{S}=\{2, 4\}$。但$\overline{S}$的逆象是$A\neq S$。

2. 假定群G与群$\overline{G}$同态，$\overline{N}$是$\overline{G}$的一个不变子群，N是$\overline{N}$的逆象。证明，$G/N\cong\overline{G}/\overline{N}$。

解 设所给G到$\overline{G}$的同态满射是

Φ: $\quad a\to\overline{a}=\Phi(a)$

我们要建立一个G/N到$\overline{G}/\overline{N}$的同构映射。定义

Ψ: $\quad aN\to\overline{a}\,\overline{N}$

若$aN=bN$，那么$b^{-1}a\in N$。由于$\overline{N}$是N在Φ之下的象，有

$$\overline{b^{-1}a}=\overline{b}^{-1}\overline{a}\in\overline{N},\qquad \overline{a}\,\overline{N}=\overline{b}\,\overline{N}$$

所以Ψ是G/N到$\overline{G}/\overline{N}$的一个映射。

设$\overline{\bar{a}N}\in\bar{G}/\bar{N}$而$\Phi(a)=\bar{a}$，那么

$$\Psi: \qquad aN\rightarrow\overline{\bar{a}\bar{N}}$$

所以Ψ是G/N到$\bar{G}/\bar{N}$的一个满射。

若$aN\neq bN$，那么$b^{-1}a\notin N$。由于N是$\bar{N}$的逆象，由此得

$$\overline{b^{-1}a}=\bar{b}^{-1}\bar{a}\notin\bar{N},\qquad \bar{a}\bar{N}\neq\bar{b}\bar{N}$$

所以Ψ是G/N与$\bar{G}/\bar{N}$间的一个一一映射。

最后，由于

$$\Psi: \qquad aNbN=abN\longrightarrow\overline{ab}\bar{N}=\bar{a}\bar{N}\bar{b}\bar{N}$$

Ψ是G/N与$\bar{G}/\bar{N}$间的一个同构映射。

3. 假定G和$\bar{G}$是两个有限循环群，它们的阶各是m和n。证明，G与$\bar{G}$同态，当而且只当$n\mid m$的时候。

解 设G与$\bar{G}$同态，那么由定理2，$G/N\cong\bar{G}$，这里N是G到$\bar{G}$的同态满射的核。所以G/N的阶是n。但G/N的阶等于不变子群N在G里的指数，所以由§9的定理2它能整除G的阶m。由此得$n\mid m$。

反过来设$n\mid m$。令$G=(a)$，$\bar{G}=(\bar{a})$。定义

$$\Phi: \qquad a^{k}\longrightarrow\bar{a}^{k}$$

若$a^{h}=a^{k}$，那么$m\mid h-k$。于是由$n\mid m$，得$n\mid h-k$而$\bar{a}^{h}=\bar{a}^{k}$。这样Φ是G到$\bar{G}$的一个映射。容易证明，Φ是G到$\bar{G}$的一个同态满射。因此G与$\bar{G}$同态。

4. 假定G是一个循环群，N是G的一个子群。证明，G/N也是循环群。

解 循环群G是交换群，所以G的子群N是不变子群，而G/N有意义。

设$G=(a)$。容易证明$G/N=(aN)$。所以G/N也是循环群。

第三章　环与域

§1. 加群、环的定义

1. 证明，本节内所给的加群的一个非空子集作成一个子群的条件是充分而且必要的。

解　可以象证明p.62定理1那样完全类似地加以证明，这里从略。

2. $R = \{0, a, b, c\}$，加法和乘法由以下两个表给定：

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\times$	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

证明，R作成一个环。

解　由加法表容易看出，R 对于加法来说，与克莱因四元群（参看第二章§9习题6）同构。因此R对于加法来说作成一个加群。

R 的乘法满足结合律：

$$(xy)z = x(yz) \qquad x, y, z \in R$$

因为当$x = 0$或a时，$(xy)z = x(yz) = 0$，当$x = b$或c时，$(xy)z = x(yz) = yz$。

两个分配律也都成立：

(1) $$x(y+z)=xy+xz$$

(2) $$(y+z)x=yx+xz$$

（1）容易验证：当$x=0$或a时

$$x(y+z)=xy+xz=0$$

当$x=b$或c时

$$x(y+z)=xy+xz=y+z$$

现在分几种情形来验证（2）。

当y和z中有一个为0时，（2）显然成立。

当$y\neq 0$，$z\neq 0$，但$y=z$时，由于R的任何元的两倍都等于0，所以（2）也成立。

当$y\neq 0$，$z\neq 0$，$y\neq z$时，有

$$(a+b)x=cx=x \qquad ax+bx=0+x=x$$

$$(b+c)x=ax=0 \qquad bx+cx=x+x=0$$

$$(c+a)x=bx=x \qquad cx+ax=x+0=x$$

由于加法满足交换律，我们已经验算了所有情形。因此（2）也成立。

这样R作成一个环。

§2. 交换律、单位元、零因子、整环

1. 证明，二项式定理

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\cdots+b^n$$

在交换环中成立。

解 对n用归纳法。当$n=1$时定理成立。设当$n=k$时定理成立：

$$(a+b)^k = a^k + \binom{k}{1}a^{k-1}b + \cdots + b^k$$

现在看 $n = k+1$的情形．由于乘法满足交换律，有

$$(a+b)^{k+1} = [a^k + \binom{k}{1}a^{k-1}b + \cdots + b^k](a+b)$$

$$= a^{k+1}[\binom{k}{1}+1]a^k b + \cdots + [\binom{k}{i} + \binom{k}{i-1}]a^{k-i+1}b^i + \cdots + b^{k+1}$$

由于 $\binom{k}{i} + \binom{k}{i-1} = \binom{k+1}{i}$ 有

$$(a+b)^{k+1} = a^{k+1} + \binom{k+1}{1}a^k b + \cdots + \binom{k+1}{i}a^{k+1-i}b^i + \cdots + b^{k+1}$$

所以二项式定理在交换环中成立。

2． 假定一个环R对于加法来说作成一个循环群．证明，R是交换环。

解 设R作为加群是由元a生成的循环群。令b和c是R的任意两个元，那么

$b = ma,\qquad c = na\qquad m$和$n$是整数

易见$bc = (mn)a^2 = cb$，因而R是交换环。

3． 证明，对于有单位元的环来说，加法适合交换律是环定义里其它条件的结果（利用$(a+b)(1+1)$）。

解 令a和b是R的任意两个元。由两个分配律得

$$(a+b)(1+1) = (a+b)\cdot 1 + (a+b)\cdot 1 = a+b+a+b$$
$$= a(1+1) + b(1+1) = a+a+b+b$$

于是有

$$(-a)+a+b+a+b+(-b) = (-a)+a+a+b+b+(-b)$$
$$b+a = a+b$$

这样就推出了加法适合交换律。

4． 找一个我们还没有提到过的有零因子的环。

解 令$R = \{(a, b,), a, b$是整数$\}$．并且定义

$$(a,\ b)=(c,\ d)\quad \text{当且仅当}\ a=c,\ b=d$$

进一步定义

$$(a,\ b)+(c,\ d)=(a+c,\ b+d)$$
$$(a,\ b)(c,\ d)=(ac,\ bd)$$

这显然是R的两个代数运算．由整数环的性质容易证明，R对于如上定义的加法和乘法作成一个环，而$(0,\ 0)$是R的零元．当$a\neq 0$，$b\neq 0$时

$$(a,\ 0)\neq(0,\ 0),\qquad (0,\ b)\neq(0,\ 0)$$

但 $(a,\ 0)(0,\ b)=(0,\ 0)$．所以R有零因子．

5． 证明，由所有实数$a+b\sqrt{2}$（a，b是整数）作成的集合R对于普通加法和乘法来说是一个整环．

解 当a，b，c，d是整数时，

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}$$

这里 $(a+c)$，$(b+d)$，$(ac+2bd)$，$(ad+bc)$仍是整数．

所以R对普通加法和乘法来说是闭的．

普通加法和乘法适合结合律、交换律和分配律．

$$(0+0\sqrt{2})=0\in R$$

对任何$a+b\sqrt{2}\in R$，有$-a-b\sqrt{2}\in R$，且

$$(a+b\sqrt{2})+(-a-b\sqrt{2})=0$$

所以R作成一个交换环，又$1+0\sqrt{2}=1\in R$，两个非零实数的乘积不等于零．

所以R是一个整环．

§3．除环、域

1． $F=\{$所有复数$a+bi$（a，b是有理数）$\}$，证明，

F对普通加法和乘法来说作成一个域

解 容易证明，F对普通加法和乘法来说作成一个整环。（参看前一节习题5．）

设$a+bi$是F的一个非零元．那么a和b不能都等于零，因而$a^2+b^2\neq 0$．容易算出，

$$(a+bi)\left(\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\right)=1$$

$$\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\in F$$

这样，F的任意非零元在F中有逆而F是一个域．

2． $F=\{$所有实数$a+b\sqrt{3}$（a，b是有理数）$\}$．证明，F对于普通加法和乘法来说是一个域．

解 容易证明，F对普通加法和乘法来说作成一个整环．设$a+b\sqrt{3}$是F的任一非零元．那么a和b不能都等于零，此时$a^2-3b^2\neq 0$．否则将有$a^2=3b^2$．若$b=0$，将得$a=0$，与假设矛盾；若$b\neq 0$，将有$\frac{a}{b}=\sqrt{3}$，与$\frac{a}{b}$是有理数矛盾．容易算出

$$(a+b\sqrt{3})\left(\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\right)=1$$

$$\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\in F$$

这样F的任意非零元在F中有逆而F是一个域．

3． 证明，一个至少有两个元而且没有零因子的有限环

R是一个除环。

解 令$R^*=\{R$的一切非零元$\}$。那么因为R至少有两个元而R^*不空。并且

Ⅰ 由于R没有零因子，所以R^*对乘法来说是闭的。

Ⅱ 乘法对R的元适合结合律，对R^*的元当然也适合。

Ⅲ 由于R没有零因子，所以消去律对R^*的元成立。

但R^*只有有限个元，所以R^*作成一个乘群。

令1是R^*的单位元，那么由于$1.0=0.1=0$，1也是R的单位元，因此R^*的元在乘群R^*中的逆也是它在R中的逆。

这样R是一个除环。

4. 证明，例3的乘法适合结合律。

解 通过简单计算即可以证明，此处从略。

5. 验证，四元数除环的任意元$(a+bi,\ c+di)$，这里a,b,c,d是实数，可以写成

$$(a,\ 0)+(b,\ 0)(i,\ o)+(c,\ 0)(0,\ 1)+(d,\ 0)(0,\ i)$$

的形式。

解

$$(b,0)(i,\ 0)=(bi,\ 0)$$
$$(c,\ 0)(0,\ 1)=(0,\ c)$$
$$(d,\ 0)(0,\ i)=(0,\ di)$$

所以

$$\begin{aligned}(a,0)+(b,0)(i,0)+(c,0)(0,1)+(d,\ 0)(0,i)\\ =(a,0)+(bi,\ 0)+(0,\ c)+(0,\ di)\\ =(a+bi,\ c+di)\end{aligned}$$

§ 4. 无零因子环的特征

1. 假定F是一个有 4 个元的域。证明：

（a） F的特征是 2；

（b） F的$\neq 0$或 1 的两个元都适合方程$x^2=x+1$。

解 （a） F的特征是F的非零元的（对加法来说的）相同的阶，并且是一个素数。F作为加群的阶是 4，因此F的非零元（对加法来说）的阶只能是 1，2 或 4 其中只有 2 是素数。所以F的特征是 2。

因此加群F与克莱因四元群B_4同构。（参看第二章§9 习题 6。）

（b） 另一方面乘群F^*的阶是 3，因而是一个循环群（a），而F^*的元是 1，a，a^2。

这样$F=\{0,1,a,a^2\}$。由于加群F与B_4同构，有

$$a+1=a^2 \qquad a^2+1=a=(a^2)^2$$

因此F的$\neq 0$或 1 的两个元a和a^2都适合方程$x^2=x+1$。

2.假定$[a]$是模n的一个剩余类。证明，若a同n互素，那么所有$[a]$的数都同n互素。（这时我们说$[a]$同n互素]。）

解 令b属于模n的剩余类$[a]$，那么

$$n|a-b \qquad a-b=ng$$

$$a=b+ng \qquad (1)$$

若$(b,n)\neq 1$，那么b和n有公因子$m>1$，于是m整除（1）式的右端，因而也整除（1）式的左端：$m|a$。这样，$(a,n)\neq 1$，与假设矛盾。这就证明了，b同n互

素。

3. 证明，所有同 n 互素的模 n 的剩余类对于剩余类的乘法来说作成一个群。（同 n 互素的剩余类的个数普通用符号 $\varphi(n)$ 来表示，并且把它叫作尤拉 φ 函数。）

解 令 $G=\{$所有同 n 互素的模 n 的剩余类$\}$。

若整数 a 和 b 都同 n 互素，那么 $a\ b$ 也同 n 互素。因此，若是 $[a]\in G$，$[b]\in G$，那么 $[a][b]\in G$，即 G 对剩余类乘法是闭的。

剩余类乘法适合结合律。

由 $(1, n)=1$ 得 $[1]\in G$ 而 G 有单位元 $[1]$。

设 $[a]\in G$。那么 $(a, n)=1$，因而存在整数 s 和 t，使

(1) $$as+nt=1$$

于是 $[a][s]+[n][t]=[1]$，但 $[n]=[0]$，所以 $[a][s]=[1]$。由(1)式显然有 $(s, n)=1$，所以 $[s]\in G$。即 G 的任何元 $[a]$ 在 G 中有逆。

这样，G 作成一个群。

4. 证明，若是 $(a, n)=1$，那么 $a^{\varphi(n)}\equiv 1\ (n)$。（费马定理。）

解 上题中群 G 的阶是 $\varphi(a)$，而 $[a]\in G$，因此

$$[a]^{\varphi(n)}=[a^{\varphi(n)}]=[1] \text{ 而 } a^{\varphi(n)}\equiv 1\ (n)$$

§5. 子环、环的同态

1. 证明，一个环的中心是一个交换子环。

解 证明很容易，此处从略。

2. 证明，一个除环的中心是一个域。

解 由上题已知一个除环D的中心Z是一个交换子环。由于Z含有单位元$1 \neq 0$，要证明Z是一个域，只须证明，若非零元$z \in Z$，那么$z^{-1} \in Z$。由$0 \neq z \in Z$得

$$az = za \qquad \text{对一切 } a \in D$$

由此得$z^{-1}azz^{-1} = z^{-1}zaz^{-1}$，$z^{-1}a = az^{-1}$ $(a \in D)$，即$z^{-1} \in Z$。

3. 证明，有理数域Q是所有复数$a+bi$（a，b是有理数）作成的域$Q(i)$的唯一的真子域。

解 由§3习题1知$Q(i)$是一个域。

Q显然是$Q(i)$的一个真子域。

设F是$Q(i)$的任一子域。那么F含有元$a \neq 0$，因而含有元$a^{-1}a = 1$。由此得F含有一切整数和一切有理数，因而含有Q：

$$Q \subset F \subset Q(i)$$

若$F \neq Q$，那么至少有一个数

$$a+bi \in F, \qquad a, b \in Q, \qquad b \neq 0$$

于是$a+bi-a = bi \in F$，$b^{-1}bi = i \in F$。由此得，F含有一切$a+bi$而$F = Q(i)$。

所以Q是$Q(i)$的唯一的真子域。

4. 证明，$Q(i)$有而且只有两个自同构映射。

解 设Φ是$Q(i)$的一个自同构。那么必然有

$$\Phi(0) = 0, \ \Phi(1) = 1, \Phi\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right), \frac{p}{q}\text{有理数}$$

考察i的象$\Phi(i)$，由

$$-1 = \Phi(-1) = \Phi(i^2) = [\Phi(i)]^2$$

得$\Phi(i) = \pm i$。因此$Q(i)$的自同构只能是

Φ_1: $a+bi \longrightarrow a+bi$

Φ_2: $a+bi \longrightarrow a-bi$

容易验证，Φ_1和Φ_2的确是$Q(i)$的自同构。

因此$Q(i)$只有两个自同构。

5. J_3表示模3的剩余类所作成的集合。找出加群J_3的所有自同构映射；再找出域J_3的所有自同构映射。

解 设Φ是加群$J_3=\{[0],[1],[2]\}$的一个自同构。那么必有$\Phi[0]=[0]$。因此加群J_3的自同构只能是

Φ_1: $[0]\longrightarrow[0]$，$[1]\longrightarrow[1]$，$[2]\longrightarrow[2]$

Φ_2: $[0]\longrightarrow[0]$，$[1]\longrightarrow[2]$，$[2]\longrightarrow[1]$

Φ_1显然是加群J_3的一个自同构。容易验证，Φ_2也是加群J_3的一个自同构。这样，加群J_3一共有Φ_1，Φ_2这两个自同构。

设Ψ是域J_3的一个自同构。那么必有

$$\Psi[0]=[0], \quad \Psi[1]=[1]$$

因而也必有$\Psi[2]=[2]$。这样的Ψ显然是域J_3的一个自同构。因此域J_3只有Ψ这个自同构。

6. 从略。

§6. 多项式环

1. 证明，假定R是一个整环，那么R上的一元多项式环$R[x]$也是一个整环。

解 已知$R[x]$是一个有单位元的交换环。要证$R[x]$是一个整环，只须证明，$R[x]$没有零因子。

设$f(x)$，$g(x)\in R[x]$，$f(x)\neq 0$，$g(x)\neq 0$。

那么$f(x)$和$g(x)$可以写成

$$f(x)=a_0+a_1x+\cdots+a_mx^m \quad (a_i\in R)$$

$$g(x)=b_0+b_1x+\cdots+b_nx^n \quad (b_i\in R)$$

的形式，这里$a_m\neq 0$，$b_n\neq 0$。于是

$$f(x)g(x)=c_0+c_1x+\cdots+a_mb_nx^{m+n} \; (c_i\in R)$$

但a_m，$b_n\in R$而R无零因子，所以$a_mb_n\neq 0$而

$$f(x)g(x)\neq 0$$

这样，$R[x]$没有零因子。

2．假定R是模7的剩类环。在$R[x]$里把乘积

$$([3]x^3+[5]x-[4])([4]x^2-x+[3])$$

计算出来。

解 $([3]x^3+[5]x-[4])([4]x^2-x+[3])$

$$=[5]x^5-[3]x^4+x^3+[5]x-[5]$$

3．证明：

(i) $R[\alpha_1,\alpha_2]=R[\alpha_2,\alpha_1]$

(ii) 若x_1，x_2，…，x_n是R上的无关未定元，那么每一个x_i都是R上的未定元。

解 (i) 由$R[\alpha_1,\alpha_2]$的定义，$\alpha_1\alpha_2=\alpha_2\alpha_1$。设

$$f(\alpha_1,\alpha_2)\in R[\alpha_1,\alpha_2]$$

那么

$$f(\alpha_1,\alpha_2)=\sum_{i_1i_2}a_{i_1i_2}\alpha_1^{i_1}\alpha_2^{i_2}$$

$$=\sum_{i_1i_2}a_{i_1i_2}\alpha_2^{i_2}\alpha_1^{i_1}\in R[\alpha_2,\alpha_1]$$

因此$R[\alpha_1,\alpha_2]\subset R[\alpha_2,\alpha_1]$。同理$R[\alpha_2,\alpha_1]\subset R[\alpha_1,\alpha_2]$。由最后两式得$R[\alpha_1,\alpha_2]=R[\alpha_2,\alpha_1]$。

(ii) 设某一x_i，例如x_1，不是R上的未定元，那么存在不全为0的a_1，a_2，…，$a_k \subset R$，使

$$a_0 + a_1 x_1 + \cdots + a_k x_1^k = 0$$

这个式子可以改写成

$$a_0 + a_1 x_1 x_2^0 \cdots x_n^0 + \cdots + a_k x_1^k x_2^0 \cdots x_n^0 = 0$$

这与x_1, x_2，…，x_n是R上无关未定元的题设矛盾。

4. 证明：

(i) 若是x_1，x_2，…，x_n和y_1，y_2，…，y_n是R上两组无关未定元，那么

$$R[x_1, x_2, \cdots, x_n] \cong R[y_1, y_2, \cdots, y_n).$$

(ii) R上的一元多项式环$R[x]$能与它的一个真子环同构。

解 (i) 对$R[x_1$，x_2，…，$x_n]$的任一元$f(x_1, x_2 \cdots, x_n)$规定

$$\Phi: \quad f(x_1, x_2, \cdots, x_n) \to$$

$$f(y_1, y_2, \cdots, y_n) \in R[y_1, y_2, \cdots, y_n]$$

我们证明，Φ是$R[x_1$，x_2，…，$x_n]$与$R[y_1$，y_2，$\cdots y_n]$间的一个同构映射。由于$R[x_1$，x_2，$\cdots x_n]$的每一元只能用一种方法写成R上的多项式$f(x_1$，x_2，…，$x_n)$，所以Φ是一个映射。由于$R[y_1$，y_2，…，$y_n]$的元也只能用一种方式写成R上的多项式$f(y_1$，y_2，…，$y_m)$，所以Φ是一个单射，容易看出，Φ也是满射，并且是一个同构映射。

(ii) x^2显然也是R上的一个未定元，并且由(i)

$$R[x^2] \cong R[x]$$

但$R[x^2] \subset R[x]$并且显然$x \bar{\in} R[x^2]$，因此$R[x^2]$是$R[x]$的一个真子集。

§7. 理 想

1. 假定R是偶数环。证明，所有整数$4r(r\in R)$是R的一个理想$\mathfrak{A}$。等式$\mathfrak{A}=(4)$对不对？

解 令$4r_1$，$4r_2$是$\mathfrak{A}$的任意两个元。由于偶数减偶数还是偶数，所以

$$4r_1-4r_2=4(r_1-r_2)\in\mathfrak{A}$$

令r是R的任意元。由于偶数乘偶数还是偶数，所以

$$r(4r_1)=(4r_1)r=4(r_1r)\in\mathfrak{A}$$

因此$\mathfrak{A}$是R的一个理想。

由于$4\in(4)$而$4\bar{\in}\mathfrak{A}$，所以$\mathfrak{A}\neq(4)$。

2. 假定R是整数环。证明，$(3,7)=(1)$。

解 由于$(3,7)$是R的理想，所以$(3,7)$含$3.2=6$以及$7-6=1$而$(1)\subset(3,7)$。但$(1)=R$，所以$(3.7)\subset(1)$。因此

$$(3,7)=(1)$$

3. 假定例3的R是有理数域。证明，这时$(2,x)$是一个主理想。

解 若R是有理数域，那么$R[x]$含有有理数$\frac{1}{2}$，因而它的理想$(2,x)$含有$\frac{1}{2}2=1$。因此$(2,x)$等于主理想(1)。

4. 证明，两个理想的交集还是一个理想。

解 从略。

5. 找出模 6 的剩余类环R的所有理想。

解 $R=\{[0], [1], [2], [3], [4], [5]\}$。若$\mathfrak{A}$是$R$的一个理想，那么$\mathfrak{A}$一定是加群$R$的一个子群。但加群$R$是循环群，所以它的子群一定也是循环群，我们有

$G_1=([0])=\{[0]\}$

$G_2=([1])=\{[5]\}=R$

$G_3=([2])=\{([4])=\{[0], [2], [4]\}$

$G_4=([3])=\{[0], [3]\}$

易见，G_1，G_2，G_3，G_4都是R的理想，因而是R的所有理想。

6. 一个环R的一个非空子集S叫作R的一个左理想，假如

(i) $a, b\in S \longrightarrow a-b\in S$

(ii) $a\in S, r\in R \longrightarrow ra\in S$

你能不能在有理数域F上的 2 × 2 矩阵环F_{22}里找到一个不是理想的左理想？

解 令S是由有理数域上一切形如

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

的矩阵组成的。易见

$$A, B\in S \Longrightarrow A-B\in S,$$

$$A\in S, L\in F_{22} \Longrightarrow LA\in S$$

所以S是F_{22}的一个左理想。若取

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\in S \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\in F_{22}$$

那么

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\notin S$$

所以S不是F_{22}的一个理想。

§8. 剩余类环、同态与理想

1. 假定我们有一个环R的一个分类，而S是由所有的类$[a]$，$[b]$，$[c]$，…所作成的集合。
又假定

$$[x]+[y]=[x+y] \qquad [x][y]=[xy]$$

规定两个S的代数运算。证明，$[0]$是R的一个理想，并且给定的类刚好是模$[0]$的R的剩余类。

解 设u，$v\in[0]$，$r\in R$。那么$[u]=[v]=[0]$。

$$[u-v]=[u]-[v]=[0]-[0]=[0]$$
$$[ru]=[r][u]=[r][0]=[0]$$
$$[ur]=[u][r]=[0][r]=[0]$$

因此$u-v\in[0]$，$ru\in[0]$，$ur\in[0]$，而$[0]$是R的一个理想。

设$[u]=[v]$。那么$[u]-[v]=[u-v]=[0]$而$u-v\in[0]$。反之，设$u-v\in[0]$，那么

$$[u]-[v]=[u-v]=[0]\text{而}[u]=[v]\text{。}$$

所以$[u]=[v]$当而且仅当$u-v\in[0]$的时候，这就是说，给定的类刚好是模$[0]$的R的剩余类。

2. 假定Φ是环R到环$\overline{R}$的一个同态满射。证明，Φ是R与$\overline{R}$间的同构映射，当而且只当Φ的核是R的零理想的时候。

解 设$\Phi(a)=\overline{a}$ $(a\in R,\ \overline{a}\in\overline{R})$。若$\Phi$是一个同构映射，那么$\Phi$是一个一一映射，因而在$\Phi$之下，只有$R$

的零元 0 是$\overline{R}$的零元$\overline{0}$的逆象，这就是说，Φ的核是R的零理想$\{0\}$。

反过来，设Φ的核是R的零理想$\{0\}$。那么R的任何一个元$c \neq 0$的象$\overline{c} \neq 0$。因此由$a \neq b$ $(a, b \in R)$ 得

$$0 \neq a - b \longrightarrow \overline{a} - \overline{b} \neq \overline{0}$$

即$\overline{a} \neq \overline{b}$而$\Phi$是一个同构映射。

3. 假定R是由所有复数$a + bi$(a, b是整数) 作成的环。环$R/(1+i)$有多少个元？

解 先看R的主理想$(1+i)$含有哪些元。

设 $a+bi \in (1+i)$。那么

$$a + bi = (x+yi)(1+i) = (x-y) + (x+y)i$$

因此，若x和y同为奇数或同为偶数，那么a和b同为偶数；若x和y一奇一偶，那么a和b同为奇数。这样，a和b必须有相同的奇偶性。反过来，设a和b有相同的奇偶性，那么方程组

$$x - y = a \qquad x + y = b$$

有整数解$x = \dfrac{a+b}{2}$，$y = \dfrac{b-a}{2}$因而$a+bi \in (1+i)$。

这样，当且仅当a和b有相同的奇偶性时，

$(a+bi) \in (1+i)$。此时$[a+bi] = [0]$

现在设a和b一奇一偶，那么

$$(a+bi) = 1 + [(a-1) + bi]$$

而$a-1$和b有相同的奇偶性。这时

$$a+bi = 1+u \qquad u \subset (1+i)$$

而$[a+bi] = [1]$，因此环$R/(1+i)$含两个元素$[0]$和$[1]$。

§9. 最大理想

1. 假定R是由所有复数$a+bi$(a, b是整数）所作成的环. 证明，$R/(1+i)$是一个域。

解 只须证明，$(1+i)$是R的一个最大理想. 设$\mathfrak{A}$是R的一个理想，并且

$$(1+i)\subset\mathfrak{A}\subset R \qquad (1+i)\neq\mathfrak{A}$$

根据这一假设，由前一节习题3，$\mathfrak{A}\ni a+bi$，此处a和b一奇一偶，因而主理想$(a+bi)\ni 1$，这样$\mathfrak{A}\ni 1$而$\mathfrak{A}=R$。

另一解法，容易看出$R/(1+i)$与模2的剩余类环同构。因此，由于2是一个素数，$R/(1+i)$是一个域。

2. 我们看环R上的一个一元多项式环$R[x]$。当R是整数环时，$R[x]$的主理想(x)是不是一个最大理想？当R是有理数域时，情形如何？

解 考察$R[x]$的理想$(2, x)$. 由于(x)的元都可以写成$f(x)x$的形式，此处$f(x)\in R[x]$，所以显然有

$$(x)\subset(2, x), \qquad 2\overline{\in}(x), \qquad (x)\neq(2, x)$$

当R是整数环时，由§7例3，$(2, x)$不是一个主理想，因而

$$(2, x)\neq(1)=R[x].$$

因此(x)不是一个最大理想。

当R是有理数域时，设$\mathfrak{A}$是$R[x]$的一个理想，并且

$$(x)\subset\mathfrak{A} \qquad (x)\neq\mathfrak{A}$$

那么

$$\mathfrak{A}\ni f(x)=a_0+a_1x+\cdots+a_nx^n, \qquad a_0\neq 0$$

由此得

$$\mathfrak{A} \ni f(x) - x(a_1 + a_2 x + \cdots + a_n x^{n-1}) = a_0$$

因此$\mathfrak{A} \ni \frac{1}{a_0} a_0 = 1$而$\mathfrak{A} = (1) = R[x]$。这就是说，在这一情形$(x)$是一个最大理想。

3. 我们看所有偶数作成的环R。证明，(4)是R的一个最大理想，但$R/(4)$不是一个域。

解 (4)刚好含有一切$4n$，这里n是整数。设$\mathfrak{A}$是R的一个理想，并且$(4) \subset \mathfrak{A}$，$(4) \neq \mathfrak{A}$。那么

$$\mathfrak{A} \ni a = 2m \neq 4n$$

由此$a = 4q + 2$，$\mathfrak{A} \ni 4q + 2 - 4q = 2$而$\mathfrak{A} = (2) = R$
这就是说，(4)是R的一个最大理想。

在$R/(4)$中，$[2] \neq [0]$ 而 $[2][2] = [4] = [0]$。因此$R/(4)$有零因子因而不是一个域。

4. 我们看有理数域F上的全部2×2矩阵环F_{22}。证明，F_{22}只有零理想和单位理想，但不是一个除环。

解 设$\mathfrak{A}$是F_{22}的一个理想并且$\mathfrak{A} \neq \{0\}$。那么$\mathfrak{A}$含有2阶矩阵$A \neq 0$。

若A的秩是2，那么A有逆A^{-1}而

$$A^{-1}A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E \in \mathfrak{A}$$

此时$\mathfrak{A} = (E) = F_{22}$。

若A的秩等于1，则存在初等矩阵P和Q，使

$$PAQ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{A}$$

容易算出

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\in \mathfrak{A}$$

因此$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}+\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=E\in \mathfrak{A}$而也有，$\mathfrak{A}=(E)=F_{22}$。这就是说，$F_{22}$只有零理想和单位理想。

但

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

所以F_{22}有零因子而不是一个除环。

§10. 商 域

1. 证明，一个域F是它自己的商域。

解 由于$F\subset F$，所以根据定理3 F含有一个F的商域Q：$Q\subset F$。但由商域的定义，有$F\subset Q$。所以$F=Q$而F是它自己的商域。

2. 详细证明本节定理3。

解 我们只须证明，在定理的证明中所做的$\bar{Q}$是域F的一个子域。

由于$\bar{Q}$是F的一个子集，$\bar{Q}$的加法和乘法是

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

$$\frac{a}{b}\ \frac{c}{d}=\frac{ac}{bd}$$

我们按照$p.97$所列的条件来验证$\bar{Q}$是F的一个子域。

$\bar{Q}$包含$\frac{a}{a}=1$，所以$\bar{Q}$包含一个不等于零的元。

$$\frac{a}{b},\ \frac{c}{d} \in \bar{Q} \Longrightarrow \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in \bar{Q}$$

$$\frac{a}{b},\ \frac{c}{d} \in \bar{Q},\ \frac{c}{d} \neq 0 \Longrightarrow \frac{a}{b}\left(\frac{c}{d}\right)^{-1} = \frac{a}{b}\ \frac{d}{c}$$

$$= \frac{a\ d}{b\ c} \in \bar{Q}$$

第四章　整环里的因子分解

§1.　素元、唯一分解

1.　证明，0不是任何元的真因子。

解　若0是元a的因子，那么$a=0.c=0$。但$0=\varepsilon.0$ (ε是单位)，所以0是0的相伴元。因此0不是$a(=0)$真因子。

2.　我们看以下的整环I：I刚好包含所有可以写成

(a)　　$\dfrac{m}{2^n}$　(m是任意整数，n是$\geqslant 0$的整数）形式

的有理数。I的哪些个元是单位，哪些个元是素元？

解　I的元总可以写成

(a)　　$2^i u$　（i整数，u奇数）

的形式。

(i)　设$\varepsilon=2^i u$是I的一个单位。那么存在ε^{-1}，使

$$\varepsilon^{-1}2^i u=1，即\ \varepsilon^{-1}=2^{-i}u^{-1}$$

于是由于I的元都有(a)的形式，必有$u=\pm 1$而$\varepsilon=\pm 2^i$。反过来，设$\varepsilon=\pm 2^i$（i整数），那么ε有逆$\varepsilon^{-1}=\pm 2^{-i}$而$\varepsilon$是$I$的单位。所以$I$的单位是一切可以写成$\pm 2^i$（$i$整数）形式的元。

(ii)　要看I的元$2^i u$是不是I的素元，由定理2只须看它的相伴元u是不是I的素元。

若奇数 u 在整数中不是素数，那么 $u=u_1u_2$，此处u_1和u_2都是不等于 ± 1 的奇数，因而由（i）都不是 I 的单位。这就是说，u 也不是 I 的素元，若奇数 u 在整数环中是一个素数而在 I 中

$$u=(2^{i_1}u_1)(2^{i_2}u_2)=2^{i_1+i_2}u_1u_2$$

此处u_1和u_2是奇数，那么必有$i_1+i_2=0$，$u=u_1u_2$。于是由于 u 是素数，u_1和u_2中必然有一个是 ± 1 而 $2^{i_1}u_1$ 和$2^{i_2}u_2$ 中必然有一个是 I 的单位。这就是说，u 也是I的素元。所以 I 的素元是一切可以写成2^iu，其中 u 是奇数的元。

3． I 是刚好包含所有复数

$$a+bi \qquad (a,\ b\text{是整数})$$

的整环。证明 5 不是 I 的素元。5 有没有唯一分解？

解 与本节的例完全类似，容易证明：

（i） I 的一个元 ε 是一个单位，当而且只 $|\varepsilon|^2=1$ 的时候。I 只有 4 个单位，就是 ± 1 和 $\pm i$。

(ii) 适合条件$|\alpha|^2=5$ 的 I 的元 α 一定是素元。

我们进一步证明。

(iii) 5 不是 I 的一个素元，并且 5 有唯一分解。

由于

$$(1) \qquad 5=(1+2\sqrt{2})(1-2\sqrt{2})$$

而$|1+2\sqrt{2}|^2=|1-2\sqrt{2}|^2=5$，所以根据($ii$)，(1)式给出了 5 的一个素元分解而 5 不是 I 的一个素元。设

$$(2) \qquad 5=\alpha_1\alpha_2\cdots\alpha_m$$

是 5 在 I 中的任一素元分解。那么由于 5 不是素元．$m\geqslant 2$。另一方面

$$|5|^2=25=|\alpha_1|^2|\alpha_2|^2\cdots|\alpha_m|^2$$

由于α_i不是单位，$|\alpha_i|^2$是不等于1的正整数，所以$m=2$而（2）必是$5=\alpha\beta$的形式，并且$|\alpha|^2=|\beta|^2=5$。由此易见，5只能有四种素元分解：

$$5=(1+2i)(1-2i)$$

$$5=(-1-2i)(-1+2i)=[-1(1+2i)][-1(1-2i)]$$

$$5=(2+i)(2-i)=[i(1-2i)][-i(1+2i)]$$

$$5=(-2-i)(-2+i)=]-i(1-2i)][i(1+2i)]$$

因此，由于±1，$\pm i$都是I的单位，5有唯一分解。

§2. 唯一分解环

1. 证明本节的推论。

解 先证：一个唯一分解环I的n个元a_1，a_2，…，a_n在I里一定有最大公因子。我们用归纳法。

当$n=2$时，由定理3，结论成立。

设$n=k-1$（$2\leqslant k-1$）时，结论成立。

看$n=k$的情形。设a_1，a_2，…，a_{k-1}的一个最大公因子是d_1而d_1，a_k的一个最大公因子是d。那么

$$d|d_1|a_1,\ a_2,\ \cdots a_{k-1},\ d|a_k$$

所以d是a_1，a_2，…，a_k的一个公因子。设c是a_1，a_2，…，a_k的任一公因子。那么$c|a_1$，a_2，…，a_{k-1}因而$c|d_1$。于是由$c|a_k$得$c|d$。所以d是a_1，a_2…，a_k的一个最大公因子。这样，结论对任何n成立。

至于a_1，a_2，…，a_n的两个最大公因子只能差一个单位因子的证明，同定理3的相应证明。

2. 假定在一个唯一分解环里

$a_1 = db_1$, $a_2 = db_2$, $\cdots$, $a_n = db_n$ (a_i不全为零)

证明：当而且只当 d 是a_1，a_2，$\cdots$，a_n的一个最大公因子的时候，b_1，b_2，$\cdots$，b_n互素。

解 假定 d 不是a_1，a_2，$\cdots$，a_n的一个最大公因子。令 c 是a_1，$a_2\cdots$，a_n的一个最大公因子。那么$d|c$，$c = dh$，此处 h 不是一个单位。于是对 $i = 1$，2，$\cdots$，n 有

$$a_i = ck_i = dhk_i = db_i$$

由于a_n不全为零，得$d \neq 0$，因而$hk_i = b_i$，即 h 是$b_1 b_2$，$\cdots$，b_n的一个非单位公因子。这就是说，b_1，$b_2\cdots$，b_n不互素。

假定 d 是a_1，a_2，$\cdots a_n$的一个最大公因子。令 t 是b_1，b_2，$\cdots$，b_n的一个公因子，那么 dt 是a_1，$a_2\cdots$，a_n的一个公因子，因而$dt|d$。由此得$t|1$，而 t 是一个单位。所以 b_1，b_2，$\cdots b_n$只有单位公因子，即b_1，b_2，$\cdots$，b_n互素。

3. 假定 I 是一个整环，(a)和(b)是I的两个主理想。证明：$(a) = (b)$ 当而且只当 b 是 a 的相伴元的时候。

解 设 $(a) = (b)$。那么 $a \in (b)$所以 $a = sb$。同样有 $b = ta$，因而 $a = sta$。若 $a = 0$，那么 $b = 0$，而 b 是 a 的一个相伴元。若 $a \neq 0$，那么 $st = 1$，t 是一个单位而 b 也是 a 的一个相伴元。

设 b 是 a 的一个相伴元，那么 $b = ta$，t 是一个单位。由此得 $(b) \subset (a)$。但 $a = t^{-1}b$，所以 $(a) \subset (b)$。这样 $(a) = (b)$。

§3. 主理想环

1. 假定I是一个主理想环，并且$(a, b)=(d)$。证明：d是a和b的一个最大公因子，因此a和b的任何最大公因子d都可以写成以下形式：

$$d=sa+tb \quad (s, t\in I)$$

解 由$(a, b)=(d)$得$a\in(d)$，$b\in(d)$。因此$d|a$，$d|b$而d是a和b的一个公因子。又由$d\in(a, b)$得$d=s'a+t'b(s', t'\in I)$。因此由$c|a$和$c|d$可得$c|p$，即a和b的任何公因子c都能整除d。所以d是a和b的一个最大公因子。

若d'是a和b的任一最大公因子，那么d'是d的相伴元：$d'=\varepsilon d$（ε是I的一个单位）。因此

$$d'=\varepsilon s'a+\varepsilon t'b=sa+tb \quad (s, t\in I)$$

2. 一个主理想环I的每一个非零最大理想都是由一个素元所生成的。

解 设(a)是I的一个非零最大理想。那么由$(a)\neq I$得a不是一个单位；由(a)非零得$a\neq 0$。若a不是一个素元，那么$a=bc$，其中b是a的一个真因子。于是$(b)\supset(a)$。但由于b不是单位，$(b)\neq I$；由于b不是a的一个相伴元，$(b)\neq(a)$。这样(a)不是I的一个最大理想，与假设矛盾。

3. 我们看两个主理想环I和I_0，这里I_0是I的一个子环。假定a和b是I_0的两个元而d是这两个元在I_0里的一个最大公因子。证明：d也是这两个元在I里的一个最大公

因子。

解 由于I_0是一个主理想环，根据题1，

$$d = sa + tb \qquad (s, t \in I_0) \tag{1}$$

在I中，d显然也是a和b的一个公因子。设c是a和b在I中的任一公因子。那么由于(1)式在I中仍然成立。c能整除(1)式的右端，因而也能整除它的左端d。这样d也是a和b在I中的一个最大公因子。

§4. 欧氏环

1. 证明，一个域F一定是一个欧氏环。

解 令$N = \{$一切≥ 0的整数$\}$。定义

$$\Phi: \qquad a \longrightarrow 1 \qquad a \in F, \qquad a \neq 0$$

那么Φ是F^*到N的一个映射。给了F^*的一个元a，F的任何元b可以写成

$$b = (ba^{-1})\, a + 0$$

所以F是一个欧氏环。

2. 看有理数域F上的一元多项式环$F[x]$。理想

$$(x^2+1,\ x^5+x^3+1)$$

等于怎样的一个主理想？

解 由于$(x^5+x^3+1) - x^3(x^2+1) = 1$，所以

$$1 \in (x^2+1,\ x^5+x^3+1)$$

由是得$(x^2+1,\ x^5+x^3+1) = (1)$。

3. 证明，由所有复数$a+bi$(a，b是整数）所作成的环R是一个欧氏环。(取$\Phi(\alpha) = |\alpha|^2$。)

解 令N是一切≥ 0的整数作成的集合而R^*是R的一

切非零元作成的集合。定义

Φ:　　　$\alpha \longrightarrow |\alpha|^2 \quad \alpha \in R^*$

那么Φ是R^*到N的一个映射。

令$\alpha = a + bi$是R^*的一个元。那么在复数域中α有逆

$$\alpha^{-1} = \frac{a - bi}{\Phi(\alpha)}$$

令$\beta = c + di$是R的任何一元。那么$\beta = (\beta\alpha^{-1})\alpha$而

$$\lambda' = \beta\alpha^{-1} = (c + di)\left(\frac{a}{\Phi(\alpha)} - \frac{b}{\Phi(\alpha)} i\right)$$

$$= k' + l' i$$

其中k'和l'是有理数。可以找到整数k和l，使

$$|k' - k| \leqslant \frac{1}{2} \quad |l' - l| \leqslant \frac{1}{2}$$

因而

$$(k' - k)^2 \leqslant \frac{1}{4} \qquad (l' - l)^2 \leqslant \frac{1}{4}$$

令$\lambda = k + li$，那么

$$\beta = \lambda'\alpha = \lambda\alpha + (\lambda' - \lambda)\alpha = \lambda\alpha + \rho$$

由于β，$\lambda\alpha \in R$，所以$\rho \in R$，这里或者$\rho = 0$或者

$$|\rho|^2 = |\lambda' - \lambda|^2 |\alpha|^2 = [(k' - k)^2 + (l' - l)^2] |\alpha|^2$$

$$\leqslant \left(\frac{1}{4} + \frac{1}{4}\right)|\alpha|^2 < |\alpha|^2$$

即$\Phi(\rho) < \Phi(\alpha)$。所以$R$是一个欧氏环。

§5. 多项式环的因子分解

1. 假定 I 是一个唯一分解环而 Q 是 I 的商域。证明，$I[x]$的一个多项式若是在$Q[x]$里可约，它在 $I[x]$ 里已经可约。

解 令 $f(x)$是 $I[x]$的一个多项式，并且在$Q[x]$里可约。$f(x)$ 可以写成 $f(x)=df_0(x)$，这里 $f_0(x)$ 是 $I[x]$的一个本原多项式。因为 d 是Q的一个单位而$f(x)$在 $Q[x]$里可约，所以$f_0(x)$在$Q[x]$里可约，于是由引理3，$f_0(x)$从而$f(x)$在 $I[x]$里可约。

2. 假定 $I[x]$是整环 I 上的一元多项式环，$f(x)$属于 $I[x]$但不属于 I，并且 $f(x)$的最高系数是 I 的一个单位。证明 $f(x)$ 在 $I[x]$里有分解。

解 (i) 首先以下简单事实成立：若 a 和 b 是 I 的元，ε 是 I 的一个单位而 $ab=\varepsilon$，那么 a 和 b 都是 I 的单位。这是因为

$$ab=\varepsilon \Longrightarrow \quad a(b\varepsilon^{-1})=1, \qquad (\varepsilon^{-1}a)b=1$$

(ii) 现在证明，$f(x)$在 $I[x]$里可以分解为有限个不可约多项式的乘积。若 $f(x)$本身是 $I[x]$ 的一个不可约多项式，那么用不着再证明什么。设 $f(x)$在$I[x]$ 里可约：

$$f(x)=g(x)h(x)$$

这里 $g(x)$和 $h(x)$ 是 $f(x)$的真因子。若$g(x)$，$h(x)$中有一个属于 I，例如 $g(x)=a\in I$，那么 a 与 $h(x)$的最高系数 b 的乘积等于 $f(x)$的最高系数 ε，这里ε 依照题设是 I 的一个单位。因此由(i)，a 也是 I 的一个单位，与

a是$f(x)$的一个真因子的假设矛盾。这样$g(x)$和$h(x)$的次数都大于零因而都小于$f(x)$的次数，并且由(i)，$g(x)$和$h(x)$的最高系数都是I的单位。因此可以同样地对$g(x)$和$h(x)$进行对$f(x)$的论证。由于$f(x)$的次数有限，最后可以在$I[x]$里把$f(x)$分解为有限个不可约多项式的乘积。

§6. 因子分解和多项式的根

1. 假定R是模16的剩余类环。$R[x]$的多项式x^2在R里有多少个根？

解 x^2在R里共有4个根，即[0],[4],[8],[12]。

2. 假定F是模3的剩余类环。看$F[x]$的多项式。

$$f(x) = x^3 - x.$$

证明，$f(a) = 0$，不管a是F的哪一个元。

解 从略。

3. 证明本节的导数规则。

解 从略。

第五章　扩域

§1.　扩域、素域

证明：$F(s)$ 的一切添加 s 的有限子集于 F 所得子域的并集 $\overline{F}$ 是一个域。

解　设 $\alpha \in F(s)$。那么

$$\alpha = \frac{f_1(\alpha_1, \alpha_2 \cdots, \alpha_n)}{f_2(\alpha_1 \alpha_2, \cdots, \alpha_n)}$$

这里 $\{\alpha_1, \alpha_2, \cdots \alpha_n\} = s_n \subset s$ 而 f_1 和 $f_2 (\neq 0)$ 是 F 上 α_1，α_2，…，α_n 的多项式。由于 s_n 是 s 的一个有限子集，因此 $\alpha \in F(s_n) \subset \overline{F}$。这就是说，$F(s) \subset \overline{F}$。反过来，显然 $\overline{F} \subset F(s)$。因此 $\overline{F} = F(s)$ 而 $\overline{F}$ 是一个域。

§2.　单扩域

1.　令 E 是域 F 的一个扩域而 $\alpha \in F$。证明，α 是 F 上一个代数元，并且 $F(\alpha) = F$。

解　$f(x) = x - \alpha$　是 $F(x)$ 的一个非零多项式，并且

$$f(\alpha) = 0$$

所以 α 是 F 上的一个代数元。

由于 $F(\alpha)$ 含 F 和 α，所以 $F \subset F(\alpha)$。

由于 F 是含 F 和 α 的一个 E 的子域而 $F(\alpha)$ 是含 F 和 α 的 E 最小子域，所以 $F(\alpha) \subset F$。

这样$F(\alpha)=F$。

2. 令F是有理数域。复数i和$\frac{2i+1}{i-1}$在F上的极小多项式各是什么？$F(i)$和$F\left(\frac{2i+1}{i-1}\right)$是否同构？

解 显然$\frac{2i+1}{i-1}\in F(i)$，因而$F\left(\frac{2i+1}{i-1}\right)\subset F(i)$。另一方面

$$\left(\frac{2i+1}{i-1}\right)^2=\frac{-3}{2i}+2\in F\left(\frac{2i+1}{i-1}\right)$$

$$\left[\left(\frac{-3}{2i}+2\right)-2\right]^{-1}\left(-\frac{3}{2}\right)=i\in F\left(\frac{2i+1}{i-1}\right)$$

因而$F(i)\subset F\left(\frac{2i+1}{i-1}\right)$。这样$F(i)=F\left(\frac{2i+1}{i-1}\right)$，因而

$$F(i)\cong F\left(\frac{2i+1}{i-1}\right)$$

F上的一次多项式$f(x)=x-a$（a是有理数）显然不能满足条件$f(i)=0$，所以i在F上的极小多项式不能是一次的。但F上的二次多项式$p(x)=x^2+1$满足条件$p(i)=0$。所以i在F上的极小多项式是x^2+1。

同样$\frac{2i+1}{i-1}$在F上的极小多项式不可能是一次的。由

$$\frac{2i+1}{i-1}=\frac{(2i+1)(i+1)}{(i-1)(i+1)}=\frac{1}{2}-\frac{3}{2}i$$

容易算出，$\frac{2i+1}{i-1}$在F上的极小多项式是$x^2-x+\frac{5}{2}$。

3. 详细证明，定理 3 中α在域F上的极小多项式是$p(x)$。

解 令$\mathfrak{A}$是$F[x]$中一切满足条件$f(\alpha)=0$的多项式$f(x)$作成的集合。由于$p(x)\in\mathfrak{A}$，所以$\mathfrak{A}$不空。设$f(x)$，$g(x)\in\mathfrak{A}$而$h(x)\in F[x]$。那么

$$f(\alpha)=0,\ g(\alpha)=0\Longrightarrow f(\alpha)-g(\alpha)=0$$
$$\Longrightarrow f(x)-g(x)\in\mathfrak{A}$$

$$f(\alpha)=0\Longrightarrow h(\alpha)f(\alpha)=0\Longrightarrow h(x)f(x)\in\mathfrak{A}$$

所以$\mathfrak{A}$是$F[x]$的一个理想。但由于$F[x]$是一个主理想环，所以$\mathfrak{A}=(p_1(x))$。由于$\mathfrak{A}\ni p(x)\neq 0$，所以$\mathfrak{A}$不是零理想而$p_1(x)\neq 0$。可以假定$p_1(x)$的最高系数是 1。但$\mathfrak{A}$中一切$f(x)$都能被$p_1(x)$整除，因此$p_1(x)$是$\mathfrak{A}$中次数最低的多项式，而它是$\alpha$在域$F$上的极小多项式。又由$p_1(x)\mid p(x)$而$p(x)$不可约，得$p(x)=cp_1(x)$，$c\in F$。但$p(x)$和$p_1(x)$的最高系数都是 1，所以$p(x)=p_1(x)$而$p(x)$是$\alpha$在$F$上的极小多项式。

4. 证明，定理 3 中的$F(\alpha)=K$。

解 由于K是域F的扩域而$\alpha\in K$，所以$F(\alpha)\subset K$。

令β是K的任一元。令K与$F[x]/p(x)$间的同构映射为Φ，而β在Φ之下的象为$\overline{\beta}$。那么

$$\overline{\beta}=\overline{b}_m\overline{x}^m+\overline{b}_{m-1}\overline{x}^{m-1}+\cdots+\overline{b}_0$$

由于在同构映射Φ之下，$\overline{\beta}$的逆象是β，$\overline{b}_i$的逆象是$b_i\in F$，$i=0, 1, \cdots, m$，$\bar{x}$的逆象是α，所以

$$\beta=b_m\alpha^m+b_{m-1}\alpha^{m-1}+\cdots+b_0$$

而$\beta\in F(\alpha)$。这样反过来有$K\subset F(\alpha)$而$F(\alpha)=K$。

§3. 代数扩域

1. 令E是域F的一个代数扩域，而α是E上的一个代数元. 证明，α是F上的一个代数元。

解 因为α是域E上的一个代数元，所以存在E上的多项式，$f(x)\neq 0$，使

$$(1)\qquad f(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_0=0\quad(a_i\in E)$$

由于E是域F的一个代数扩域，所以a_n都是F上代数元，而E的子域$E'=F(a_0, a_1, \cdots, a_n)$是$F$上一个有限扩域。但由(1)，$\alpha$显然是$E'$上一个代数元。所以$E'(\alpha)$是$E'$上一个有限扩域因而是$F$上一个有限扩域。这样

$$E'(\alpha)=F(a_0, a_1, \cdots, a_{n-1}, \alpha)$$

是F上一个代数扩域而α是F上一个代数元。

2. 令F，I和E是三个域并且$F\subset I\subset E$。假定

$$(I:F)=m$$

而E的元α在F上的次数是n，并且$(m, n)=1$。证明，α在I上的次数也是n。

解 由于α在F上的次数是n，所以α在F上的极小多项式$p(x)$的次数是n。设α在I上的极小多项式$p_1(x)$的次数是s。那么由于$p(x)$也是I上的多项式，得$p_1(x)|$

$p(x)$而 $s \leqslant n$。设 $I(\alpha)$在$F(\alpha)$ 上的次数为 t。那么

$$(I(\alpha):F)=(I(\alpha):F(\alpha))(F(\alpha):F)=tn$$

$$(I(\alpha):F)=(I(\alpha):I)(I:F)=sm$$

因此$tn=sm$而 $n\mid sm$。但 $(m, n)=1$，所以$n\mid s$。

由 $s\leqslant n$和$n\mid s$得 $s=n$。这就是说，α在I上的次数也是n。

3. 令域F的特征不是2，E是F的一个扩域，并且

$$(E:F)=4$$

证明，存在一个满足条件$F\subset I\subset E$ 的F的二次扩域I的充分与必要条件是：$E=F(\alpha)$ 而α在F上的极小多项式是

$$x^4+ax^2+b$$

解 先证条件是充分的。设$E=F(\alpha)$而α在F上的极小多项式是x^4+ax^2+b。那么令$I=F(\alpha^2)$，就显然有$F\subset I\subset E$。由于x^4+ax^2+b在F上不可约，所以x^2+ax+b在F上也不可约。但

$$(\alpha^2)^2+a(\alpha^2)+b=\alpha^4+a\alpha^2+b=0$$

所以x^2+ax+b是α^2在F上的极小多项式而I是F的二次扩域。

现在反过来证明条件是必要的。设

$$F\subset I\subset E \qquad (I:F)=2 \qquad (E:F)=4$$

(i) 显然有$(E:I)=2$。取$\theta\in E$，$\theta\notin I$，那么θ在I上的次数是2。设θ在I上的极小多项式是$x^2+\beta x+\gamma$，那么

$$\theta^2+\beta\theta+\gamma=0 \qquad \beta,\ \gamma\in I$$

由于F的特征不是2，$\theta+\frac{\beta}{2}$有意义。我们有

$$\left(\theta+\frac{\beta}{2}\right)^2=\theta^2+\beta\theta+\frac{\beta^2}{4}+\gamma-\gamma=\frac{\beta^2}{4}-\gamma$$

令 $\omega=\theta+\frac{\beta}{2}$，$\delta=\frac{\beta^2}{4}-\gamma$，那么 $E=I(\omega)$ 而 ω 在 I 上的极小多项式是 $x^2-\delta(\delta\in I)$。

(ii) 设 $\delta\bar{\in}F$，那么 δ 在 F 上的极小多项式是

$$x^2+ax+b \qquad (a, b\in F)$$

由于 $\omega^2=\delta$，所以 $\omega^4+a\omega^2+b=0$。但

$$I=F(\delta),\ E=I(\omega)=F(\delta, \omega)=F(\omega)$$

而 $(E:F)=4$，所以 ω 在 F 上的极小多项式是 x^4+ax^2+b。

(iii) 若 $\delta\in F$，那么由于 $(I:F)=2$，与（i）平行可以找到 $\lambda\in I$，$\lambda\bar{\in}F$ 而 $\lambda^2\in F$。取 $\omega'=\omega(1+\lambda)$。那么

$$\omega'^2=\omega^2(1+2\lambda+\lambda^2)$$

由于 $\omega^2=\delta\in F$ 而 $1+2\lambda+\lambda^2\bar{\in}F$，所以 $\omega'^2=\delta'\bar{\in}F$。于是与(ii) 一样有 $E=F(\omega')$ 而 ω' 在 F 上的极小多项式是

$$x^4+ax^2+b。$$

4. 令 E 是域 F 的一个有限扩域。那么总存在 E 的有限个元 α_1，α_2，…，α_m，使

$$E=F(\alpha_1, \alpha_2, \cdots, \alpha_m)$$

解 设 $(E:F)=m$。那么 E 作为 F 上向量空间有一组基 α_1，α_2，…，α_m。显然

$$E=F(\alpha_1, \alpha_2, \cdots, \alpha_m)$$

5. 令 F 是有理数域，看添加复数于 F 所得扩域

$$E_1=F\left(2^{\frac{1}{3}}, 2^{\frac{1}{3}}i\right)$$

$$E_2=F\left(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}\omega i\right),\quad \omega=\frac{-1+\sqrt{3}\,i}{2},\quad \omega^3=1$$

证明：

$$\left(E_1:F\left(2^{\frac{1}{3}}\right)\right)=2\qquad (E_1:F)=6$$

$$\left(E_2:F\left(2^{\frac{1}{3}}\right)\right)=4\qquad (E_2:F)=12$$

解 $E_1=F\left(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}i\right)=F\left(2^{\frac{1}{3}},\ i\right)\supset F\left(2^{\frac{1}{3}}\right)\supset F$

因为 $i\notin F\left(2^{\frac{1}{3}}\right)$ 而 i 是 x^2+1 的根，所以 $\left(E_1:F\left(2^{\frac{1}{3}}\right)\right)=2$。

因为 $2^{\frac{1}{3}}\notin F$ 而 $2^{\frac{1}{3}}$ 是 F 上不可约多项式 x^3-2 的一个根，所以 $F\left(2^{\frac{1}{3}}\right)$ 是 F 上一个 3 次扩域。因此

$$(F_1:F)=\left(E_1:F\left(2^{\frac{1}{3}}\right)\right)\left(F\left(2^{\frac{1}{3}}\right):F\right)=2\times 3=6$$

由 $E_2=F\left(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}\omega i\right)$ 得 $\omega i\in E_2$，$-(\omega i)^3=i\in E_2$。

于是由 $\omega=\frac{-1+\sqrt{3}}{2}i$ 得 $\sqrt{3}\in E_2$。所以

$$E_2=F\left(2^{\frac{1}{3}},\sqrt{3},\ i\right)\supset F\left(2^{\frac{1}{3}},\sqrt{3}\right)\supset F\left(2^{\frac{1}{3}}\right)\supset F$$

易见 $(E_2 : F(2^{\frac{1}{3}}, \sqrt{3})) = 2$。但$\sqrt{3} \notin F(2^{\frac{1}{3}})$。否则

$$F(2^{\frac{1}{3}}) \supset F(\sqrt{3}) \supset F$$

而 $(F(2^{\frac{1}{3}}) : F) = 3$，$(F(\sqrt{3}) : F) = 2$，与定理 1 矛盾．这样

$$(F(2^{\frac{1}{3}}, \sqrt{3}) : F(2^{\frac{1}{3}})) = 2 \qquad (E_2 : F(2^{\frac{1}{3}})) = 4$$

于是由 $(F(2^{\frac{1}{3}}) : F) = 3$ 得 $(E_2 : F) = 12$。

§4． 多项式的分裂域

1． 证明，有理数域F上多项式x^4+1的分裂域是一个单扩域$F(\alpha)$，其中α是x^4+1的一个根。

解 在复数域C里

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

所以在C里x^4+1的 4 个根是

$$\alpha_1 = \frac{\sqrt{2}}{2}(1+i),\ \alpha_2 = \frac{\sqrt{2}}{2}(1-i),$$

$$\alpha_3 = -\alpha_1,\ \alpha_4 = -\alpha_2$$

由于$\alpha_2 = -\alpha_1^3$，得$F(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = F(\alpha_1)$，所以单扩域$F(\alpha_1)$就是$x^4+1$在$F$上的分裂域。

2． 令F是有理数域，$x^3 - a$是F上一个不可约多项式而α是$x^3 - a$的一个根。证明，$F(\alpha)$不是$x^3 - a$在F上的分裂域。

解　x^3-a的三个根是$a^{\frac{1}{3}}$，$a^{\frac{1}{3}}\omega$，$a^{\frac{1}{3}}\omega^2$，其中

$$\omega=\frac{-1+\sqrt{3}i}{2}\qquad \omega^3=1$$

x^3-a在F上的分裂域是

$$E=F(a^{\frac{1}{3}},\ a^{\frac{1}{3}}\omega,\ a^{\frac{1}{3}}\omega^2)=F(a^{\frac{1}{3}},\ \omega)$$

我们有$F(a^{\frac{1}{3}},\ \omega)\supset F(a^{\frac{1}{3}})\supset F$. 由于$\omega$不属于$F(a^{\frac{1}{3}})$而$\omega$是$F(a^{\frac{1}{3}})$上多项式$x^2+x+1$的根，所以

$$(F(a^{\frac{1}{3}},\ \omega):F(a^{\frac{1}{3}}))=2$$

又由于$a^{\frac{1}{3}}$是F上不可约多项式x^3-a的根，所以

$$(F(a^{\frac{1}{3}}):F)=3$$

因此$(E:F)=6$。令α是多项式x^3-a的任一根。那么$(F(\alpha):F)=3$。所以$E\neq F(\alpha)$，即$F(\alpha)$不是x^3-a在F上的分裂域。

3．令$p_1(x)$，$p_2(x)$，…，$p_m(x)$是域F上m个最高系数为1的不可约多项式. 证明，存在F的一个有限扩域

$$F(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m)$$

其中α_i在F上的极小多项式是$p_i(x)$。

解　令$f(x)=p_1(x)p_2(x)\cdots p_m(x)$。做$f(x)$在域$F$上的分裂域$E$。$E$含有$f(x)$的所有根，因而含有$\alpha_1$，$\alpha_2$，…，$\alpha_m$，其中$\alpha_i$各是$p_i(x)$的一个根，$i=1$，2，…$m$。因此

$$E\supset F(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m)$$

由于 $p_1(x)\cdots$, $p_m(x)$都是F上最高系数为1的不可约多项式，所以它们分别是α_1, α_2, …, α_m在F上的极小多项式。由于α_1, α_2, …, α_m 都是F上的代数元,所以$F(\alpha_1, \alpha_2, \cdots, \alpha_m)$ 是F上的一个有限扩域。

4. 令P是一个特征为素数p的域，$F=P(\alpha)$ 是P的一个单扩域，而α是$P[x]$的多项式x^p-a的一个根。$P(\alpha)$ 是不是x^p-a在P上的分裂域?

解 由于α是x^p-a的一个根，所以$\alpha^p=a$。但域P因而域F的特征是p，所以在$F[x]$中

$$x^p-a=x^p-\alpha^p=(x-\alpha)^p$$

这样$P(\alpha)$是添加x^p-a的p个相同的根于P而得到的，因此$P(\alpha)$是x^p-a在P上的分裂域。

§5. 有限域

1. 令F是一个含p^n个元的有限域.证明,对于n的每一个因数$m>0$，存在并且只存在F的一个有p^m个元的子域L。

解 令F所含素域为Δ，那么根据本节定理2，F是多项式$x^{p^n}-x$在Δ上的分裂域，若正整数m整除n：$n=md$，那么$p^n-1=(p^m)^d-1$，因而$p^m-1\mid p^n-1$：$p^n-1=(p^m-1)t$。于是

$$x^{p^n}-x=x(x^{p^n-1}-1)=x[(x^{p^m-1})^t-1]$$

由此得$x^{p^m-1}-1\mid x^{p^n-1}-1$，即$x^{p^m}-x\mid x^{p^n}-x$.但$F$含$x^{p^n}-x$的所有根，因此$F$也含$x^{p^m}-x$的所有根。由定理3的证

明，这些根作成一个有 p^m 个元的F的子域L。若 L_1 也是一个有 p^m 个元的F的子域，那么根据定理2，L_1 也是由 $x^{p^m}-x$ 在F中的所有根作成的，因而 $L_1=L$。

2. 一个有限域一定有比它大的代数扩域。

解 令F是一个含有 p^n 个元的有限域。在F上做多项式 $x^{p^{2n}}-x$ 的分裂域E，那么$F\subset E$，并且E是F的一个代数扩域。但E至少含有多项式 $x^{p^{2n}}-x$ 的 p^{2n} 个不同的根，因此E大于F。

读者可以自己证明，E实际上是 $x^{p^{2n}}-x$ 在F所含素域Δ上的分裂域。

3. 令F是一个有限域，Δ是它所含素域并且 $F=\Delta(\alpha)$。α是否必须是F的非零元所作成的乘群的一个生成元？

解 令Δ是特征为3的素域，它的元用0，1，2来表示。这三个元都不是 $f(x)=x^2+1$ 的根，所以$f(x)$是Δ上的一个不可约多项式。做Δ上单代数扩域 $F=\Delta(\alpha)$，其中α在Δ上的极小多项式是$f(x)$。那么F有9个元而F的非零元所作成的乘群F^*的阶是8。但

$$\alpha^2=-1 \qquad \alpha^4=1$$

所以α不是F^*的一个生成元。

4. 令Δ是特征为2的素域。找出$\Delta[x]$的一切三次不可约多项式。

解 因为Δ只有两个元0和1，而$\Delta[x]$的常数项为0的三次多项式显然可约，所以$\Delta[x]$最多有以下4个三次不可约的多项式：

$$x^3+x^2+x+1,\ x^3+x^2+1,\ x^3+x+1,\ x^3+1$$

但1是x^3+x^3+x+1和x^3+1的根，所以这两个多项式在Δ上可约。因为0和1都不是x^3+x^2+1和x^3+x+1的根，所以只有后两个多项式是$\Delta[x]$的不可约多项式。

§6. 可离扩域

1. 令域F的特征是p，$f(x)$是F上一个不可约多项式，并且$f(x)$可以写成F上x^{p^e}但不能写成$x^{p^{e+1}}$的多项式（$e\geqslant 1$）。证明，$f(x)$的每一个根的重复度都是p^e。

解 设$f(x)=g(x^{p^e})$，这里$g(x)$是F上一个多项式。由于$f(x)$在F上不可约，并且$f(x)$不能写成F上$x^{p^{e+1}}$的多项式，所以$g(x)$在F上不可约并且不能写成F上x^p的多项式。因此由引理1，$g(x)$没有重根。令E是多项式$f(x)$ $g(x)$在F上的一个分裂域、那么在E里

$$g(x)=a_m(x-\beta_1)(x-\beta_2)\cdots(x-\beta_m)$$

这里$a_m\in F$，$\beta_i\in E$，$i=1,2,\cdots,m$，并且当$i\neq j$时，$\beta_i\neq\beta_j$。而

$$f(x)=g(x^{p^e})=a_m(x^{p^e}-\beta_1)(x^{p^e}-\beta_2)\cdots(x^{p^e}-\beta_m)$$

令α是$f(x)$在E里的任何一个根，那么

$$(1)\qquad f(\alpha)=a_m(\alpha^{p^e}-\beta_1)(\alpha^{p^e}-\beta_2)\cdots(\alpha^{p^e}-\beta_m)=0$$

由于β_i（$i=1,2,\cdots,m$）各不相等，(1)式中只有一个因子

$$\alpha^{p^e}-\beta_i=0,\ \text{即}\ \alpha^{p^e}=\beta_i$$

由于$f(x)$在E中完全分解，所以在E中有$f(x)$的m个

不同的根α_i，使$\alpha_i^{p^e}=\beta_i\,(i=1,\ 2,\ \cdots,\ m)$。这样

$$f(x)=a_m(x^{p^e}-\alpha_1^{p^e})(x^{p^e}-\alpha_2^{p^e})\cdots(x^{p^e}-\alpha_m^{p^e})$$

$$=a_m(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_m)^{p^e}$$

因而$f(x)$的每一个根的重复度都是p^e。

2. 设域F没有不可离扩域。证明，F的任一代数扩域都没有不可离扩域。

解 设E是F的一个代数扩域而α是E上的一个代数元。令α在E上的极小多项式是

$$f(x)=x^n+\beta_{n-1}x^{n-1}+\cdots+\beta_0$$

那么由于E是F的代数扩域，β_0，…，β_{n-1}都是F上的代数元。于是α是F上有限扩域$F(\beta_0,\ \cdots,\ \beta_{n-1})$的代数元，因而也是$F$上的代数元。但$F$没有不可离扩域，所以$\alpha$是$F$上可离元，而$\alpha$在$F$上的极小多项式$g(x)$没有重根。但$f(x)\,|\,g(x)$，所以$f(x)$也没有重根，而$\alpha$是$E$上的可离元。这样，$E$上的任意代数元都是$E$上的可离元，即$E$没有不可离扩域。

3. 令域F的特征是p而$E=F(\alpha,\ \beta)$，这里α是F上n次可离元，而β是F上p次非可离元。$(E:F)=?$

解 按照题设，β在F上的极小多项式$f(x)$的次数是p。令β在$F(\alpha)$上的极小多项式是$h(x)$，那么$h(x)\,|\,f(x)$，因而$h(x)$的次数$\leqslant p$。

设 $h(x)$的次数小于p。那么$h(x)$不能写成$g(x^p)$的形式，这里$g(x)$是$F(\alpha)[x]$的一个多项式。因此β是$F(\alpha)$上的一个可离元。但α是F上一个可离元，所以根据引理4，β也是F上一个可离元，与β是F上一个非可离元

的题设矛盾。这样，$h(x)$的次数是 p。于是有

$$(F(\alpha,\ \beta):F(\alpha))=p,\quad (F(\alpha):F)=n,$$

$$(E:F)=(F(\alpha,\ \beta):F(\alpha))(F(\alpha):F)=pn$$

4. 找一个域 F，使 F 有一个有限扩域 E 而 E 不是F 的单扩域。

解 令 Δ 是特征为 2 的素域，$F=\Delta(x,\ y)$，这里x和y是 F 上两个无关未定元。考察 $E=F\ (\sqrt{x},\sqrt{y})$，这里 $\sqrt{x}$ 和$\sqrt{y}$在 F 上的极小多项式各是

$$z^2-x \text{ 和 } z^2-y$$

由于$\sqrt{y}\notin F(\sqrt{x})$，所以$\sqrt{y}$在$F(\sqrt{x})$上的极小多项式仍是 z^2-y、这样

$$(E:F(\sqrt{x}))=2,(F(\sqrt{x}):F)=2,(E:F)=4$$

E 的任一元 α 都可以写成 F上$\sqrt{x}$和$\sqrt{y}$的多项式：

$$\alpha=f(\sqrt{x},\ \sqrt{y})$$

由于F 的特征是 2，这样一个多项式的二次方等于它的各项的二次方的和，因而 $\alpha^2=g(x,\ y)$，这里 $g(x,\ y)$ 是 F 上 x 和 y 的多项式。因此 $\alpha^2\in F$。这就是说，E 的任一元α 在 F 上的次数最多是 2。这样，F上四次扩域 E 不可能是一个单扩域 $F(\alpha)$。